

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-304752

(P2004-304752A)

(43) 公開日 平成16年10月28日 (2004. 10. 28)

(51) Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
H04 L 12/66	H04 L 12/66 B	5 B089
G06 F 13/00	G06 F 13/00 351 Z	5 K030

審査請求 有 請求項の数 107 O L (全 125 頁)

(21) 出願番号 特願2003-295020 (P2003-295020)  
(22) 出願日 平成15年8月19日 (2003. 8. 19)  
(31) 優先権主張番号 特願2002-238989 (P2002-238989)  
(32) 優先日 平成14年8月20日 (2002. 8. 20)  
(33) 優先権主張国 日本国 (JP)  
(31) 優先権主張番号 特願2003-74781 (P2003-74781)  
(32) 優先日 平成15年3月19日 (2003. 3. 19)  
(33) 優先権主張国 日本国 (JP)

特許法第30条第1項適用申請有り

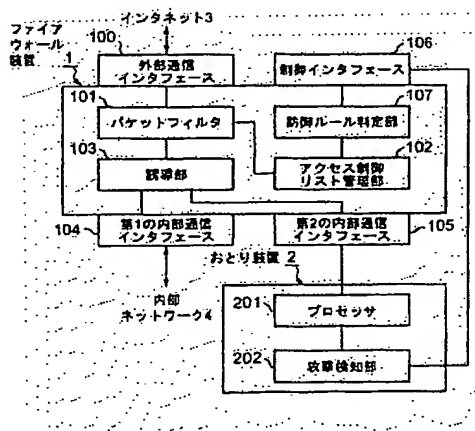
(71) 出願人 000004237  
日本電気株式会社  
東京都港区芝五丁目7番1号  
(74) 代理人 100097157  
弁理士 桂木 雄二  
(72) 発明者 中江 政行  
東京都港区芝五丁目7番1号 日本電気株  
式会社内  
(72) 発明者 山形 昌也  
東京都港区芝五丁目7番1号 日本電気株  
式会社内  
Fターム (参考) 5B089 HA10 KA05 KA17 KB06 KC21  
KC37  
5K030 GA15 HA08 HB11 HD03 HD06  
LB05 MA04

(54) 【発明の名称】 攻撃防御システムおよび攻撃防御方法

(57) 【要約】

【課題】 インターネットから内部ネットワークへのアクセスでSSLなど通信路暗号化技術が用いられた場合であって不正なアクセスを検知し有効に防御する攻撃防御システム及び方法を提供する。

【解決手段】 ファイアウォール装置1およびおとり装置2を備え、ファイアウォール装置1では、受け取ったIPパケットのヘッダ情報を参照し、所定のルールに基づいて攻撃の可能性がある「不審パケット」をおとり装置2へと誘導する。おとり装置2は、サービスを提供するプロセスを監視しながら、攻撃の有無を判定する。攻撃を検出した際には、攻撃元ホストのIPアドレスを含むアラートを生成してファイアウォール装置1に伝達する。当該アラートを受けたファイアウォール装置1は、以降、攻撃元ホストからのIPパケットの受入れを拒否する。



## 【特許請求の範囲】

## 【請求項1】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記おとり装置は、

前記ファイアウォール装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記ファイアウォール装置は、

入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とする攻撃防御システム。

## 【請求項2】

入力IPパケットの前記ヘッダ情報は当該入力IPパケットの送信元IPアドレスおよび宛先IPアドレスの少なくとも一方であり、

前記転送先選択手段は前記入力IPパケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力IPパケットの転送先を決定する、

ことを特徴とする請求項1記載の攻撃防御システム。

## 【請求項3】

前記転送先選択手段は、

前記内部ネットワークで使用されていないIPアドレスからなる誘導リストを前記振り分け条件として保持する格納手段を有し、

前記入力IPパケットの宛先IPアドレスと前記誘導リスト内の未使用IPアドレスとが一致したときに当該入力IPパケットを前記おとり装置へ転送する、

ことを特徴とする請求項1記載の攻撃防御システム。

## 【請求項4】

前記転送先選択手段は、

入力IPパケットを格納するパケットバッファと、

前記入力IPパケットを前記内部ネットワークに転送し、宛先到達不能メッセージを受信するか否かを監視する監視手段と、

を有し、

前記監視手段が宛先到達不能メッセージを受信した場合、対応する入力IPパケットを前記パケットバッファから前記おとり装置へ転送することを特徴とする請求項1記載の攻撃防御システム。

## 【請求項5】

前記ファイアウォール装置は、前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、前記振り分け条件を更新する振り分け条件更新手段をさらに有することを特徴とする請求項1記載の攻撃防御システム。

## 【請求項6】

前記フィルタリング条件管理手段は、前記おとり装置へ転送した入力IPパケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、前記入力IPパケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を前記パケットフィルタリング手段へ返すことを特徴とする請求項1記載の攻撃防御システム。

## 【請求項7】

前記フィルタリング条件管理手段は、

前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力IPパケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、

前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、

を有することを特徴とする請求項1ないし6のいずれかに記載の攻撃防御システム。

## 【請求項8】

前記おとり装置は、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生滅に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とする請求項1記載の攻撃防御システム。

## 【請求項9】

前記おとり装置は、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項1記載の攻撃防御システム。

## 【請求項10】

前記おとり装置は、さらに、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項8に記載の攻撃防御システム。

## 【請求項11】

前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少

なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項10記載の攻撃防御システム。

#### 【請求項12】

前記内部ネットワーク上のサーバから前記おとり装置へ少なくともファイルシステムを複写するミラーリング装置をさらに有し、

前記おとり装置で攻撃が検知されると、前記ミラーリング装置は前記内部ネットワーク上のサーバから少なくともファイルシステムを前記おとり装置へ複写することを特徴とする請求項1記載の攻撃防御システム。

#### 【請求項13】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする攻撃防御システム。

#### 【請求項14】

前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度を更新することを特徴とする請求項13記載の攻撃防御システム。

#### 【請求項15】

前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に所定数を加算することを特徴とする請求項14記載の攻撃防御システム。

#### 【請求項16】

前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に対応する入力IPパケットのパケットサイズが大きくなるほど値が小さくなる変数を、当該信頼度に加算することを特徴とする請求項14記載の攻撃防御システム。

#### 【請求項17】

前記信頼度管理手段は、前記入力IPパケットが予め定められたプロトコルのパケットである場合のみ信頼度の更新を実行することを特徴とする請求項14記載の攻撃防御システム。

#### 【請求項18】

前記信頼度管理手段は、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度と当該信頼度の最終更新時刻とを格納するための第1信頼度格納手段と、

前記第1信頼度格納手段の内容の複製を格納するための第2信頼度格納手段と、

前記信頼度格納手段に格納されたある信頼度が前記転送先選択手段によって取得されるごとに、当該信頼度を更新する第1更新処理手段と、

前記第1信頼度格納手段の内容を定期的に複製して前記第2信頼度格納手段へ格納するための複製処理手段と、

前記第2信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する第2更新処理手段と、

を有することを特徴とする請求項13記載の攻撃防御システム。

#### 【請求項19】

前記複製処理手段は、前記第1信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を有するエントリを前記第1信頼度格納手段から削除することを特徴とする請求項18記載の攻撃防御システム。

#### 【請求項20】

前記第2更新処理手段は、前記最終更新時刻から所定期間が経過した信頼度を所定値だけ低下させることを特徴とする請求項18記載の攻撃防御システム。

#### 【請求項21】

前記第2更新処理手段は、前記最終更新時刻から所定期間が経過した信頼度を前記第2更新処理手段から削除することを特徴とする請求項18記載の攻撃防御システム。

#### 【請求項22】

前記おとり装置は、前記ファイアウォール装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有することを特徴とする請求項13記載の攻撃防御システム。

#### 【請求項23】

前記信頼度管理手段は、前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに応じて、当該入力IPパケットの送信元IPアドレスの信頼度を更新することを特徴とする請求項22記載の攻撃防御システム。

#### 【請求項24】

前記おとり装置は、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生成に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果

関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とする請求項 13 記載の攻撃防御システム。

【請求項 25】

前記おとり装置は、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項 13 記載の攻撃防御システム。

【請求項 26】

前記おとり装置は、さらに、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項 24 に記載の攻撃防御システム。

【請求項 27】

前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項 26 記載の攻撃防御システム。

【請求項 28】

前記内部ネットワーク上のサーバから前記おとり装置へ少なくともファイルシステムを複製するミラーリング装置をさらに有し、

前記おとり装置で攻撃が検知されると、前記ミラーリング装置は前記内部ネットワーク上のサーバから少なくともファイルシステムを前記おとり装置へ複製することを特徴とする請求項 13 記載の攻撃防御システム。

【請求項 29】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

第 1 転送先選択手段と、

第 2 転送先選択手段と、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第 1 転送先選択手段は、入力 IP パケットのヘッダ情報および第 1 所定条件に基づいて、当該入力 IP パケットを前記第 2 転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第 2 転送先選択手段は、前記第 1 転送先選択手段から転送された前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第 2 所定条件を満たすか否かに応じて当該入力 IP パケットの転送先を前記内部ネットワーク及び

前記おとり装置のいずれかに決定する、

ことを特徴とする攻撃防御システム。

【請求項 30】

前記おとり装置は、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生滅に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とする請求項 29 記載の攻撃防御システム。

【請求項 31】

前記おとり装置は、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項 29 記載の攻撃防御システム。

【請求項 32】

前記おとり装置は、さらに、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項 30 に記載の攻撃防御システム。

【請求項 33】

前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項 32 記載の攻撃防御システム。

【請求項 34】

前記おとり装置および前記ファイアウォール装置は単一ユニットに収容されていることを特徴とする請求項 29 のいずれかに記載の攻撃防御システム。

【請求項 35】

前記内部ネットワーク上のサーバから前記おとり装置へ少なくともファイルシステムを複製するミラーリング装置をさらに有し、

前記おとり装置で攻撃が検知されると、前記ミラーリング装置は前記内部ネットワーク上のサーバから少なくともファイルシステムを前記おとり装置へ複製することを特徴とする請求項 29 記載の攻撃防御システム。

【請求項 36】

内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

IP パケットのフィルタリング条件および振り分け条件を用意し、



入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定し、

受理された入力IPパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項37】

入力IPパケットの前記ヘッダ情報は当該入力IPパケットの送信元IPアドレスおよび宛先IPアドレスの少なくとも一方であり、

前記入力IPパケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力IPパケットの転送先を決定することを特徴とする請求項36記載の攻撃防御方法。

【請求項38】

前記振り分け条件は、前記内部ネットワークで使用されていないIPアドレスからなる誘導リストであり、

前記入力IPパケットの宛先IPアドレスと前記誘導リスト内の未使用IPアドレスとが一致したときに当該入力IPパケットを前記おとり装置へ転送することを特徴とする請求項36記載の攻撃防御方法。

【請求項39】

攻撃を検知したか否かに基づいて、前記振り分け条件を更新するステップをさらに有することを特徴とする請求項36記載の攻撃防御方法。

【請求項40】

前記フィルタリング条件管理ステップは、

前記おとり装置へ転送した入力IPパケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、

前記入力IPパケットに対応するフィルタリング条件の有効期限が経過している場合には、デフォルトのフィルタリング条件を設定する、

ことを特徴とする請求項36記載の攻撃防御方法。

【請求項41】

前記フィルタリング条件管理ステップは、

攻撃を検知した際の攻撃カテゴリと当該入力IPパケットのアドレス情報とに対応したフィルタリング条件を生成し、

生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新する、

ことを特徴とする請求項36記載の攻撃防御方法。

【請求項42】

前記攻撃の有無を検知するステップは、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けを行うことを特徴とする請求項36記載の攻撃検知方法。

【請求項43】

前記攻撃の有無を検知するステップは、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを抽出し、

当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ことを特徴とする請求項36記載の攻撃検知方法。

【請求項44】

さらに、前記イベントとドメイン制約またはタイプ制約を付加したルールとを照合することを特徴とする請求項42記載の攻撃検知方法。

【請求項45】

ドメイン制約またはタイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生源となったネットワーク受信イベントとを抽出することを特徴とする請求項44記載の攻撃検知方法。

【請求項46】

前記ルールは、ネットワークドメインを含むアクセス元に関する制約と、アクセスを処理するプロセスまたはその系列に関する制約と、を記述したことを特徴とする請求項43または44に記載の攻撃検知方法。

【請求項47】

内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

IPパケットの振り分け条件を用意し、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を保持し、

入力IPパケットの送信元IPアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御方法。

【請求項48】

前記信頼度を保持するステップは、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度と当該信頼度の最終更新時刻とをリアルタイム信頼度データベースに格納し、

前記リアルタイム信頼度データベースに格納されたある信頼度がアクセスされるごとに当該信頼度を更新し、

前記リアルタイム信頼度データベースの内容を定期的

に複製して長期信頼度データベースに格納し、

前記長期信頼度データベースに格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する、

ステップを有することを特徴とする請求項 47 記載の攻撃防御方法。

#### 【請求項 49】

前記おとり装置において、前記ファイアウォール装置から転送された入力 IP パケットに対するサービスプロセスを実行することで攻撃の有無を検知するステップをさらに有することを特徴とする請求項 47 記載の攻撃防御方法。

#### 【請求項 50】

攻撃が検知されたか否かに応じて、当該入力 IP パケットの送信元 IP アドレスの信頼度を更新するステップをさらに有することを特徴とする請求項 49 記載の攻撃防御方法。

#### 【請求項 51】

前記攻撃の有無を検知するステップは、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生成と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けを行うことを特徴とする請求項 49 記載の攻撃検知方法。

#### 【請求項 52】

前記攻撃の有無を検知するステップは、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生成と、に係るイベントを抽出し、

当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ことを特徴とする請求項 49 記載の攻撃検知方法。

#### 【請求項 53】

さらに、前記イベントとドメイン制約またはタイプ制約を付加したルールとを照合することを特徴とする請求項 51 記載の攻撃検知方法。

#### 【請求項 54】

ドメイン制約またはタイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントとを抽出することを特徴とする請求項 53 記載の攻撃検知方法。

#### 【請求項 55】

前記ルールは、ネットワークドメインを含むアクセス元に関する制約と、アクセスを処理するプロセスまたはその系列に関する制約と、を記述したことを特徴とする請求項 52 または 53 に記載の攻撃検知方法。

#### 【請求項 56】

内部ネットワークと外部ネットワークとの境界に設置さ

れ、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力 IP パケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力 IP パケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力 IP パケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とするファイアウォール装置。

#### 【請求項 57】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力 IP パケットのヘッダ情報および振り分け条件に基づいて、当該入力 IP パケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力 IP パケットの転送先を決定することを特徴とするファイアウォール装置。

#### 【請求項 58】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

第 1 転送先選択手段と、

第 2 転送先選択手段と、

複数の入力 IP パケットにおける各送信元 IP アドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第 1 転送先選択手段は、入力 IP パケットのヘッダ情報および第 1 所定条件に基づいて、当該入力 IP パケットを前記第 2 転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第 2 転送先選択手段は、前記第 1 転送先選択手段から転送された前記入力 IP パケットの送信元 IP アドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第 2 所定条件を満たすか否かに応じて当該入力 IP パケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定することを特徴とするファイアウォール装置。

## 【請求項59】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、

前記おとり装置へ転送した入力IPパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とするファイアウォール装置。

## 【請求項60】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御システムを実装するためのプログラムにおいて、

IPパケットのフィルタリング条件および振り分け条件を用意し、

入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定し、

受理された入力IPパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

## 【請求項61】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御システムを実装するためのプログラムにおいて、

IPパケットの振り分け条件を用意し、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を保持し、

入力IPパケットの送信元IPアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御プログラム。

## 【請求項62】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IPパケットのフィルタリング条件および振り分け条件を用意し、

入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定し、

受理された入力IPパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に対して、転送した入力IPパケットに対するサービスプロセスを実行させることで攻撃の有無を検知させ、前記おとり装置が攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とするプログラム。

## 【請求項63】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

IPパケットの振り分け条件を用意し、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を保持し、

入力IPパケットの送信元IPアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とするプログラム。

## 【請求項64】

攻撃防御システムのおとり装置において、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生成に係るイベントを一時的に記憶するイベント記憶手段と、

前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とするおとり装置。

## 【請求項65】

攻撃防御システムのおとり装置において、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とするおとり装置。

【請求項66】

さらに、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段と、

を有することを特徴とする請求項64に記載のおとり装置。

【請求項67】

前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項66記載のおとり装置。

【請求項68】

内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

入力IPパケットに含まれる要求データおよび振り分け条件に基づいて、当該入力IPパケットの転送先として、前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

要求データの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力IPパケットに含まれる要求データに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする攻撃防御システム。

【請求項69】

前記転送先選択手段は、前記信頼度管理手段から得られた入力IPパケットに含まれる要求データに対する信頼度が、所定の閾値以上の場合に、前記内部ネットワークおよび前記おとり装置の双方に当該入力IPパケットを転送することを特徴とする請求項68記載の攻撃防御システム。

【請求項70】

前記転送先選択手段は、前記信頼度管理手段から得られた入力IPパケットに含まれる要求データに対する信頼度が、所定の閾値よりも小さい場合に、当該入力IPパケットを一時的に記憶する入力バッファを有し、

前記おとり装置において前記要求データが安全であることを確認した場合に、前記入力IPパケットは前記

力バッファから前記内部ネットワークに自動的に再転送されることを特徴とする請求項68または69に記載の攻撃防御システム。

【請求項71】

前記おとり装置は、

サービスプロセスの実行において、少なくともネットワーク入出力、ファイル入出力、および、プロセス生滅に係るイベントを一時的に記憶するイベント記憶手段と、

10 前記イベント記憶手段に記憶されたイベント間の因果関係を分析して、リンク付けを行うイベント管理手段と、

を有することを特徴とする請求項68記載の攻撃防御システム。

【請求項72】

前記おとり装置は、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項68記載の攻撃防御システム。

20

【請求項73】

前記おとり装置は、さらに、

ドメイン制約およびタイプ制約の少なくとも一方を付加したルールにしたがって、前記サービスプロセスの実行状況から攻撃を検知する攻撃検知手段を有することを特徴とする請求項71に記載の攻撃防御システム。

【請求項74】

前記攻撃検知手段は、前記ドメイン制約および前記タイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントと、を抽出することを特徴とする請求項73記載の攻撃防御システム。

30

【請求項75】

前記ファイアウォール装置において、

暗号化された入力IPパケットを復号するとともに、出力IPパケットを暗号化するための暗号処理手段を備えたことを特徴とする前記請求項68ないし70のいずれかに記載の攻撃防御システム。

40

【請求項76】

前記内部ネットワーク上のサーバから前記おとり装置へ少なくともファイルシステムを複製するミラーリング装置をさらに有し、

前記おとり装置で攻撃が検知されると、前記ミラーリング装置は前記内部ネットワーク上のサーバから少なくともファイルシステムを前記おとり装置へ複製することを特徴とする請求項68記載の攻撃防御システム。

【請求項77】

攻撃防御システムの攻撃検知方法において、

50

サービスプロセスを実行させながら、少なくともネッ

トワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、イベント間の因果関係を分析してリンク付けを行う、ことを特徴とする攻撃検知方法。

【請求項78】

攻撃防御システムの攻撃検知方法において、サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを抽出し、当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、ことを特徴とする攻撃検知方法。

【請求項79】

さらに、前記イベントとドメイン制約またはタイプ制約を付加したルールとを照合することを特徴とする請求項77記載の攻撃検知方法。

【請求項80】

ドメイン制約またはタイプ制約を判定するにあたり、前記リンクを走査して、少なくとも、検査対象であるイベントの発生源となったプロセスの生成イベントと、イベントの発生原因となったネットワーク受信イベントとを抽出することを特徴とする請求項79記載の攻撃検知方法。

【請求項81】

前記ルールは、ネットワークドメインを含むアクセス元に関する制約と、アクセスを処理するプロセスまたはその系列に関する制約と、を記述したことを特徴とする請求項78または79に記載の攻撃検知方法。

【請求項82】

内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

I Pパケットのフィルタリング条件および振り分け条件を用意し、

入力I Pパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力I Pパケットを受理するか否かを判定し、

受理された入力I Pパケットに含まれる要求データおよび前記振り分け条件に基づいて、当該入力I Pパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力I Pパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力I Pパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項83】

前記振り分け条件は、要求データとその信頼度との組からなる信頼度管理テーブルであり、

前記入力I Pパケットに含まれる要求データと、前記信頼度管理テーブルのあるエントリ内の要求データとが一致した場合は、当該エントリ内の信頼度を抽出し、

前記信頼度管理テーブル内に前記入力I Pパケットに含まれる要求データに一致するエントリがない場合には、当該要求データと信頼度の初期値との組である新たなエントリを作成する、

ステップを有することを特徴とする請求項82記載の攻撃防御方法。

【請求項84】

前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値以上である場合に、前記内部ネットワークおよび前記おとり装置の双方を選択する、

ステップを有することを特徴とする請求項82または83に記載の攻撃防御方法。

【請求項85】

前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値よりも小さい場合に、前記入力I Pパケットを一時的に記憶し、

攻撃が検知されなかった後に、当該入力I Pパケットを内部ネットワークに自動的に転送する、

ステップを有することを特徴とする請求項82または83に記載の攻撃防御方法。

【請求項86】

コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けを行う、ステップを有することを特徴とする攻撃検知プログラム。

【請求項87】

コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを抽出し、

当該イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ステップを有することを特徴とする攻撃検知プログラム。

【請求項88】

コンピュータに、攻撃防御システムの攻撃検知を実行させるためのプログラムにおいて、

サービスプロセスを実行させながら、少なくともネットワーク入出力と、ファイル入出力と、プロセス生滅と、に係るイベントを一時的に記憶し、

イベント間の因果関係を分析してリンク付けし、

前記イベントと、ドメイン制約またはタイプ制約を付加したルールと、を照合する、

ステップを有することを特徴とする攻撃検知プログラム。

【請求項89】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御を実行させるためのプログラムにおいて、

IPパケットのフィルタリング条件および振り分け条件を用意し、

入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定し、

受理された入力IPパケットに含まれる要求データおよび前記振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力IPパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項90】

前記振り分け条件は、要求データとその信頼度との組からなる信頼度管理テーブルであり、

前記入力IPパケットに含まれる要求データと、前記信頼度管理テーブルのあるエントリ内の要求データとが一致した場合は、当該エントリ内の信頼度を抽出し、

前記信頼度管理テーブル内に前記入力IPパケットに含まれる要求データに一致するエントリがない場合には、当該要求データと信頼度の初期値との組である新たなエントリを作成する、

ステップを有することを特徴とする請求項89記載の攻撃防御プログラム。

【請求項91】

前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値以上である場合に、前記内部ネットワークおよび前記おとり装置の双方を選択する、

ステップを有することを特徴とする請求項89または90に記載の攻撃防御プログラム。

【請求項92】

前記転送先の決定において、前記信頼度管理テーブルから抽出された信頼度が、所定の閾値よりも小さい場合に、前記入力IPパケットを一時的に記憶し、

攻撃が検知されなかった後に、当該入力IPパケットを内部ネットワークに自動的に転送する、

ステップを有することを特徴とする請求項89または90に記載の攻撃防御プログラム。

【請求項93】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、

おとり装置と、

ファイアウォール装置と、

前記おとり装置と前記ファイアウォール装置との間に接続されたスイッチ装置と、

を有し、

前記おとり装置は、

前記スイッチ装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記スイッチ装置は、

前記ファイアウォール装置で受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力IPパケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、を有し、

前記ファイアウォール装置は、

前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、

入力IPパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、を有する、

ことを特徴とする攻撃防御システム。

【請求項94】

前記スイッチ装置は、さらに、

複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段を有し、

前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする請求項93記載の攻撃防御システム。

【請求項95】

前記ファイアウォール装置および前記スイッチ装置はネットワーク接続されていることを特徴とする請求項93記載の攻撃防御システム。

【請求項96】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、

前記内部ネットワーク内の特定のサーバ装置に対応す

る複数のおとり装置を含むおとりクラスタと、

前記特定サーバ装置および前記複数のおとり装置へ選択的に入力IPパケットを転送するファイアウォール装置と、

を有し、

前記ファイアウォール装置は、

入力IPパケットに対する信頼度を管理するための信頼度管理手段と、

前記おとりクラスタ内の各おとり装置に少なくとも1種類の必須信頼度を割り当てて管理するサーバ管理手段と、

を有し、あるIPパケットを入力すると、当該入力IPパケットに対する信頼度を前記信頼度管理手段から取得し、当該信頼度以下の必須信頼度を有するおとり装置を当該入力IPパケットの転送先として決定することを特徴とする攻撃防御システム。

【請求項97】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、

ファイアウォール装置と、

前記内部ネットワークおよび前記外部ネットワークの少なくとも一方に設けられた少なくとも1つの攻撃検知システムと、

を有し、

前記ファイアウォール装置は、前記少なくとも1つの攻撃検知システムから攻撃検知アラートを受信し、少なくとも攻撃元IPアドレスおよび攻撃先IPアドレスを含むアラートに変換するアラート変換手段を有することを特徴とする攻撃防御システム。

【請求項98】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、

ファイアウォール装置と、

おとり装置と、

少なくとも1つの信頼性管理サーバと、

を有し、

前記ファイアウォール装置は入力IPパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、

前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力IPパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、

ことを特徴とする攻撃防御システム。

【請求項99】

前記ファイアウォール装置は、

入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択

する転送先選択手段と、

前記少なくとも1つの信頼度管理サーバ装置に対して前記要求メッセージを送信し、その応答として前記入力IPパケットの信頼度を取得するための管理サーバ接続手段と、

を有し、

前記転送先選択手段は、前記信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする請求項98記載の攻撃防御システム。

【請求項100】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおける攻撃防御方法において、

前記内部ネットワーク内の特定のサーバ装置に対応する複数のおとり装置を用意し、

前記複数のおとり装置の各々に割り当てられた少なくとも1種類の必須信頼度に基づくIPパケットの振り分け条件と、複数の入力IPパケットに対する信頼度と、を保持し、

あるIPパケットを入力すると、当該入力IPパケットに対する信頼度を取得し、

前記信頼度以下の必須信頼度を有するおとり装置を当該入力IPパケットの転送先として決定する、

ことを特徴とする攻撃防御方法。

【請求項101】

内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおける攻撃防御方法において、

前記内部ネットワークおよび前記外部ネットワークの少なくとも一方に少なくとも1つの攻撃検知システムを用意し、

前記少なくとも1つの攻撃検知システムから攻撃検知アラートを受信すると、少なくとも攻撃元IPアドレスおよび攻撃先IPアドレスを含むアラートに変換する、ことを特徴とする攻撃防御方法。

【請求項102】

コンピュータに、内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムを実装するためのプログラムにおいて、

前記内部ネットワーク内の特定のサーバ装置に対応して設けられた複数のおとり装置の各々に少なくとも1種類の必須信頼度を割り当て、

前記必須信頼度に基づくIPパケットの振り分け条件と複数の入力IPパケットに対する信頼度とを保持し、

あるIPパケットを入力すると、当該入力IPパケットに対する信頼度を取得し、

前記信頼度以下の必須信頼度を有するおとり装置を当該入力IPパケットの転送先として決定する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項103】



コンピュータに、内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムを実装するためのプログラムにおいて、

前記内部ネットワークおよび前記外部ネットワークの少なくとも一方に設けられた少なくとも1つの攻撃検知システムから攻撃検知アラートを受信し、

前記受信した攻撃検知アラートを少なくとも攻撃元IPアドレスおよび攻撃先IPアドレスを含むアラートに変換する、

ステップを有することを特徴とする攻撃防御プログラム。 10

#### 【請求項104】

内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも1つの信頼性管理サーバと、を有する攻撃防御システムにおける攻撃防御方法において、

前記ファイアウォール装置は入力IPパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、

前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力IPパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、

ステップを有することを特徴とする攻撃防御方法。

#### 【請求項105】

前記ファイアウォール装置は、前記応答メッセージに含まれる信頼度が所定の振り分け条件を満たすか否かに応じて、前記入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする請求項104記載の攻撃防御方法。

#### 【請求項106】

内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも1つの信頼性管理サーバと、を有する攻撃防御システムにおける前記信頼性管理サーバをコンピュータに実装するためのプログラムにおいて、

前記ファイアウォール装置から入力IPパケットもしくはその一部のデータを含む要求メッセージを受信し、

前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力IPパケットに対する信頼度を生成し、

前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、

ステップを有することを特徴とする信頼度管理プログラム。

#### 【請求項107】

コンピュータに、内部ネットワークと外部ネットワーク 50

との境界に設置され、少なくともファイアウォール装置と信頼度管理サーバとを用いた攻撃防御システムを実装するためのプログラムにおいて、

入力IPパケットもしくはその一部のデータを含む要求メッセージを前記ファイアウォール装置から前記信頼性管理サーバへ送信し、

前記要求メッセージに含まれるデータから算出された前記入力IPパケットに対する信頼度を少なくとも含む応答メッセージを前記信頼性管理サーバから受信し、

前記応答メッセージに含まれる信頼度が所定の振り分け条件を満たすか否かに応じて、前記入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御プログラム。

#### 【発明の詳細な説明】

#### 【技術分野】

#### 【0001】

本発明はコンピュータネットワークにおけるセキュリティ対策に係り、特に外部ネットワークからの攻撃に対して内部ネットワーク上の資源を保護するためのシステムおよび方法に関する。

#### 【背景技術】

#### 【0002】

従来、外部ネットワークからの攻撃に対する防御技術として、(1)ファイアウォール、(2)侵入検知システム、(3)おとりシステム、といった手法があった。

#### 【0003】

ファイアウォールの一例は、たとえば特開平8-44642号公報(特許文献1)に開示されている。外部のIPネットワークと内部のイーサネット(登録商標)との境界にファイアウォールを設置し、検査対象となるパケットを外部ネットワークから内部ネットワークに通過させてよいか否かを判定する。特に、ファイアウォールにパケットフィルタを設け、パケットのヘッダ情報(送信元アドレスや送信先アドレス)などの他、プロトコルの種別(TCP/UDP/HTTPなど)や、データ内容(ペイロード)なども参照しながら、所定のルールに従って、パケットの通過可否を判定する。適切なルールを設定しておけば、例えば、外部ネットワーク一般に公開されているWebサーバなどに対してワームなどを含む不正なパケットが進入することを遮断できる。

#### 【0004】

侵入検知システムの一例は、たとえば特開2001-350678号公報(特許文献2)に開示されている。この従来の侵入検知システムは不正侵入判定ルール実行部を有し、アプリケーションごとの判定ルール、例えばWWWサーバ用不正侵入判定ルールやMAILサーバ用不正侵入判定ルールを備えている。まず、IPアドレステーブル取得部は、内部ネットワーク上を流れるパケッ



トの送信元 IP アドレスもしくは送信先 IP アドレスから、当該 IP アドレスを持つサーバにおいて現在動作中のアプリケーションを決定する。次に、不正侵入判定ルール実行部において、そのアプリケーションに応じた不正侵入判定ルールを実行し、当該パケットが不正であるか否かを判定する。こうすることにより、アプリケーションに依存したより精度の高い侵入検知が可能となる。

#### 【0005】

おとりシステムの第 1 例は、たとえば特開 2000-261483 号公報（特許文献 3）に開示されている。この従来のおとりシステムは、ルータ 10 の下に構築された内部ネットワーク上に、トラフィック監視装置、攻撃パターンおよび偽装サーバを備える。まず、トラフィック監視装置において、内部ネットワーク上を流れるパケットを監視しながら、特定の攻撃パターンに合致するものを不正パケットとして検出し、その識別情報（送信元 IP アドレス、送信先 IP アドレスなどを含む）をルータに通知する。次に、ルータでは、後に続く外部ネットワークからのパケットについて、検出した識別情報に合致するパケットをすべて偽装サーバに転送する。偽装サーバは、転送されたパケットを適切に解釈し、内部ネットワーク上の正規のサーバをまねた偽の応答パケットを生成し、先に不正パケットを送信したホストへ向けて、その偽の応答パケットを送信する。こうすることで、外部ネットワーク上に存在する攻撃者に、内部ネットワークに悪影響のない形で、攻撃を続けさせることができ、逆探知によって攻撃者の身元を明らかにすることができる。

#### 【0006】

おとりシステムの第 2 例は、たとえば特開 2002-7234 号公報（特許文献 4）に開示されている。この従来のおとりシステムは、内部ネットワークと外部ネットワーク（インターネット）との境界に、いわゆるゲートウェイとして、不正検出サーバと、おとりサーバと、を備える。外部ネットワークから内部ネットワークへ流れるパケットを不正検出サーバで監視し、例えば、当該パケットのペイロードについて所定のパターンマッチング処理を行うなどして、不正か否かを判定する。不正であると判定されたパケットには、その旨を示す特殊なマークを加えた上で、当該パケットをおとりサーバもしくは内部ネットワーク上の情報処理サーバへ転送する。情報処理サーバへ不正パケットを転送する場合、予め情報処理サーバに不正回避処理部を持たせておき、特殊なマークのあるパケットを受信した際には、さらにおとりサーバへ当該パケットを転送するようにしておく。いずれにせよ、不正検出サーバで検出された不正パケットは、最終的におとりサーバへ到達する。その後、おとりサーバでは、偽の応答パケットを生成し、不正パケットの送信元ホストに向けて、当該応答パケットを送信する。こうすることで、不正と判定されたパケットを全ておとり

サーバに閉じ込めることができる。

#### 【0007】

さらに、おとりシステムの第 3 例は、たとえば特開平 09-224053 号公報（特許文献 5）に記載されている。この従来のおとりシステムは、公衆ネットワーク（インターネット）と、プライベートネットワーク（内部ネットワーク）との境界に、スクリーン・システムおよび代行ネットワークを備える。スクリーン・システムは、自身に接続される各ネットワークからの着信パケットについて、パケットのヘッダに記載される情報や着信履歴など基にしたスクリーン基準に従い、フィルタリングを行う。ただし、スクリーン・システムの通信インタフェースは IP アドレスをもたず、traceroute などを用いた探索から自身を隠蔽することを特徴の 1 つとする。もう 1 つの特徴として、プライベートネットワークに向かう着信パケットについて、代行ネットワークに経路を変更することもできる。代行ネットワーク上には 0 台以上の代行ホストが設けられ、プライベートネットワーク上にあるホストの代理として動作させることもできる。こうすることで、公衆ネットワークからの攻撃からプライベートネットワークを保護できる。

#### 【0008】

【特許文献 1】特開平 8-44642 号公報（段落番号 0029～0030、図 5）

【特許文献 2】特開 2001-350678 号公報（段落番号 0062～0084、図 1）

【特許文献 3】特開 2000-261483 号公報（段落番号 0024～0030、図 1）

【特許文献 4】特開 2002-7234 号公報（段落番号 0036～0040、図 1、図 2）

【特許文献 5】特開平 09-224053 号公報（段落番号 0037～0043、0066～0067、図 6）。

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0009】

しかしながら、上記従来技術は、いずれも、次に挙げるような問題点を持つ。

#### 【0010】

第 1 の問題点は、外部ネットワーク上の攻撃ホストと内部ネットワーク上のサーバとの間で、SSL（Secure Socket Layer）や IPsec（RFC 2401 記載）などの通信路暗号化技術が用いられた場合に、攻撃を有効に検知または防御できないということである。その理由は、攻撃検知のための主要なデータ（ペイロードなど）が暗号化されており参照できないためである。

#### 【0011】

第 2 の問題点は、攻撃検知部のパフォーマンスが、近年のネットワークの高速化に追いつききれず、検査から漏

れるパケットが存在したり、ネットワークの高速性を損なったりする点にある。その理由は、攻撃検知の精度を向上するには、より多彩な、あるいはより複雑な判定ルールの実行が必要であるが、一方、ネットワークの高速化により、検査対象となるパケット量が飛躍的に増加しているためである。

#### 【0012】

また、特許文献2および特許文献3に記載された侵入検知システムやおとりシステムの第1例では、少なくとも1つの不正パケットが、内部ネットワーク上の保護すべきサーバに到達してしまう。その理由は、攻撃検知部が検査を行うのは、パケットのコピーでしかなく、当該パケットが不正と判定された場合でも、その内部ネットワーク上のパケット流通を遮断できないためである。

#### 【0013】

さらに、特許文献5に記載されたおとりシステムの第3例では、インターネットから到来したパケットを代行ネットワークに経路変更させる条件および方法については検討されていない。このために、正確にパケットを振り分けることができず、正常なアクセスが代行ネットワークへ、異常なアクセスが内部ネットワークへ導かれる可能性がある。

#### 【0014】

第3の問題点は、攻撃検知精度の向上が困難な点にある。近年のサーバ運用の形態は、遠隔からの保守作業が一般的であり、その作業はサーバ内のデータ修正やシステムの更新などであり、侵入検知システムはこうした保守作業をしばしば攻撃と誤って検知してしまう。

#### 【0015】

また、Webアプリケーション等で知られるように、サーバのサブシステムとして、データベース操作など様々なアプリケーションプログラムを動作させることが多く、そうしたサブシステムの脆弱性を突いて不正動作を行わせる攻撃も頻繁に見られるようになった。侵入検知システムは、一般によく知られるサーバまたはそのサブシステムへの攻撃パターンを知識として備えるが、サイト独自に作成されたサブシステムが存在する場合や、一般的なサーバまたはサブシステムであっても設定に不備がある場合には、前記攻撃パターンに当てはまらない、いわゆる未知攻撃を受ける危険性がある。

#### 【0016】

第4の問題点は、データベースやプラグインモジュールなどのサブシステムを備えるサーバシステムにおいて、クライアントとの通信プロトコルで、一定のアクセス手順が規定されている場合（すなわちステートフルプロトコルであった場合）、不審なアクセスのみをおとりサーバなど、正規のサーバ以外に誘導する方法では、おとりサーバと正規のサーバ双方でクライアントーサーバ通信が失敗する。特に、誤っておとりサーバへ誘導されたアクセスがあった場合には、正規のサーバ上であるべ

き処理が行われないため、サーバ障害を発生させることになる。

#### 【0017】

本発明の目的は、通信路暗号化技術を用いた通信システムに対しても、外部ネットワークからの攻撃を有効に防御できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

#### 【0018】

本発明の他の目的は、高速ネットワーク環境に対応できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

#### 【0019】

本発明のさらに他の目的は、保護すべきサーバに向けられた不正パケットを確実に遮断できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

#### 【課題を解決するための手段】

#### 【0020】

本発明の第1の観点によれば、おとり装置およびファイアウォール装置を含む攻撃防御システムが内部ネットワークと外部ネットワークとの境界に設置され、おとり装置はファイアウォール装置から転送された入力IPパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、ファイアウォール装置は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、前記おとり装置へ転送した入力IPパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有することを特徴とする。

#### 【0021】

本発明の第2の観点によれば、ファイアウォール装置は、入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、を有し、前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする。

#### 【0022】

本発明による攻撃防御方法は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入

力IPパケットの受理および廃棄のいずれかを実行し、受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、前記入力IPパケットが前記おとり装置へ転送されると、当該入力IPパケットに対するサービスプロセスを実行し、前記サービスプロセスの実行状況を監視しながら、所定の攻撃カテゴリと関連づけられたルールに違反するか否かを判定することで攻撃の有無を検知し、前記入力IPパケットに関して攻撃を検知したか否かに応じて、当該入力IPパケットのヘッダ情報に対応するフィルタリング条件を設定し、入力したIPパケットのヘッダ情報に対応するフィルタリング条件に従ってパケットフィルタリングを実行する、ステップを有することを特徴とする。

#### 【0023】

望ましくは、本発明によるファイアウォール装置は、入力IPパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力IPパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力IPパケットのヘッダ情報および振り分け条件に基づいて当該入力IPパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力IPパケットにおける各送信元IPアドレスの信頼度を管理するための信頼度管理手段と、前記おとり装置へ転送した入力IPパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて当該入力IPパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有し、前記転送先選択手段は、前記入力IPパケットの送信元IPアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特徴とする。

#### 【0024】

本発明の第3の観点によれば、おとり装置は、プロセスから伝達される各プロセス状況について、その発生原因となった過去のプロセス状況を関連付けた上で、時系列順にメモリに格納するイベント管理手段を有することを特徴とする。さらに、プロセス状況の正常・異常を判定する際に、前記関連付けを探索して、関連プロセス状況列を分析する攻撃検知手段を有し、攻撃検知手段はプロセス状況の発生源であるプロセスと、その親プロセスとの関係、さらにアクセス元IPアドレスとの関係などの制約の下で、当該プロセス状況の正常・異常を判定することを特徴とする。

#### 【0025】

本発明の第4の観点によれば、ファイアウォール装置は、サーバもしくはそのサブシステムへの要求などを含むアプリケーションデータと、おとり装置における過去

の攻撃検知結果とを組にして格納するハッシュ表管理部と、入力IPパケットのペイロードを参照して、アプリケーションデータを抽出し、前記ハッシュ表管理部に当該アプリケーションデータの登録状況などを問い合わせ、その結果に応じて、前記内部ネットワークおよび前記おとり装置のいずれか、またはその双方を当該入力IPパケットの転送先として選択する転送先選択手段と、を有し、前記転送先選択手段は、ハッシュ表管理部におけるアプリケーションデータの登録有無や、登録があった場合に攻撃として検知されているかどうかを確認して、登録がない場合もしくは過去に攻撃として検知されているアプリケーションデータをおとり装置へ誘導し、それ以外の場合には、内部ネットワークとおとり装置の双方へ転送することを特徴とする。

#### 【0026】

本発明の第5の観点によれば、内部ネットワーク内の特定のサーバ装置に対応する複数のおとり装置を含むおとりクラスタを設け、ファイアウォール装置は、おとりクラスタ内の各おとり装置に少なくとも1種類の必須信頼度を割り当てて管理し、入力IPパケットに対する信頼度を取得すると、当該信頼度以下の必須信頼度を有するおとり装置を当該入力IPパケットの転送先として決定することを特徴とする。

#### 【0027】

本発明の第6の観点によれば、内部ネットワークおよび外部ネットワークの少なくとも一方に設けられた少なくとも1つの攻撃検知システムを有し、ファイアウォール装置は、少なくとも1つの攻撃検知システムから攻撃検知アラートを受信し、少なくとも攻撃元IPアドレスおよび攻撃先IPアドレスを含むアラートに変換するアラート変換手段を有することを特徴とする。

#### 【0028】

本発明の第7の観点によれば、ファイアウォール装置と、おとり装置と、少なくとも1つの信頼性管理サーバと、を有し、ファイアウォール装置は入力IPパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力IPパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信することを特徴とする。さらに、ファイアウォール装置は、入力IPパケットのヘッダ情報および振り分け条件に基づいて、当該入力IPパケットの転送先として内部ネットワークおよびおとり装置のいずれかを選択する転送先選択手段と、少なくとも1つの信頼度管理サーバ装置に対して要求メッセージを送信し、その応答として入力IPパケットの信頼度を取得するための管理サーバ接続手段と、を有し、転送先選択手段は信頼度が振り分け条件を満たすか否かに応じて当該入力IPパケットの転送先を決定することを特

徴とする。

【発明の効果】

【0029】

以上詳細に説明したように、本発明による攻撃防御システム及び方法によれば、IPパケットのヘッダ情報に基づいてパケットの誘導を行うために、外部ネットワークから内部ネットワークへのアクセスにおいて通信路暗号化技術が用いられた場合でも、攻撃を検知および防御することができる。いかなる通信路暗号化技術が用いられたとしても、少なくともIPヘッダに記載されたソースIPアドレスもしくはディスティネーションIPアドレスは暗号化されず、さらにファイアウォール装置によるおとり装置への誘導は、これらIPヘッダに記載された情報を基に行うことができるためである。

【0030】

また、本発明によれば、ファイアウォール装置によるおとり装置への誘導方法が少ないパラメータを基にした簡易なアルゴリズムで実現できるため、高速ネットワーク環境においても、ネットワーク性能を高いレベルで維持できる。

【0031】

さらに、本発明によれば、おとり装置へ誘導されて攻撃が検出された全てのパケットについて、その送信元ホストからの以降のアクセスを拒否するように動的な防御を行うことで後続する攻撃を全てファイアウォール装置で防御することができる。このために内部ネットワークへの通信経路が無くなり、検出された攻撃用パケットが一切内部ネットワークに到達しない。

【発明を実施するための最良の形態】

【0032】

(ネットワーク構成)

図1は、本発明による攻撃防御システムの概略的ブロック図である。本発明による攻撃防御システムは、基本的に、ファイアウォール装置1およびおとり装置2を有し、インターネット3と内部ネットワーク4との境界にファイアウォール装置1が設置されている。内部ネットワーク4は、WWW (World-Wide Web) などのサービスを提供する1個以上のサーバ装置401を含む。ここではインターネット3に攻撃元ホスト301が想定されている。

【0033】

ファイアウォール装置1は、通常の正規のパケットであれば、これを通過させて内部ネットワーク4へ送付し、不正パケットあるいは不審なパケットであれば、おとり装置2へ誘導する。おとり装置2は攻撃の有無を検知し、攻撃を検知した場合にはアラートをファイアウォール装置1へ出力する。また、不正パケットに対する偽の応答パケットを生成してファイアウォール装置1へ返してもよい。ファイアウォール装置1はその偽の応答パケットを不正パケットの送信元である攻撃元ホスト30

1へ送信する。

【0034】

(第1実施形態)

1. 1) 構成

図2は、本発明の第1実施形態による攻撃防御システムのファイアウォール装置1およびおとり装置2の構成を示すブロック図である。ファイアウォール装置1は、外部通信インタフェース100でインターネット3と接続され、第1の内部通信インタフェース104で内部ネットワーク4と接続される。

【0035】

パケットフィルタ101は、外部通信インタフェース100および誘導部103の間に接続され、アクセス制御リスト管理部102から取得したアクセス制御ルールに従ってパケットフィルタリングを行う。すなわち、後述するように、パケットフィルタ101は外部通信インタフェース100および誘導部103の一方から受け取ったIPパケットを他方へ転送し、あるいは転送せずに廃棄する。

20 【0036】

パケットフィルタ101で受理されたパケットは誘導部103へ送られ、誘導部103は、後述する誘導リスト(図5)を参照し、パケットフィルタ101から入力したIPパケットの宛先IPアドレスに応じて当該パケットを第1の内部通信インタフェース104および第2の内部通信インタフェース105のいずれかへ誘導する。逆に、第1の内部通信インタフェース104または第2の内部通信インタフェース105からインターネット3に向かうIPパケットをパケットフィルタ101に転送する。

30 【0037】

第1の内部通信インタフェース104は、誘導部103から入力したIPパケットを内部ネットワーク4に伝達し、内部ネットワーク4からインターネット3に向かうIPパケットを誘導部103へ伝達する。第2の内部通信インタフェース105は、誘導部103によって誘導されたIPパケットをおとり装置2に伝達し、おとり装置2からインターネット3に向かうIPパケットを誘導部103に伝達する。

40 【0038】

おとり装置2は、プロセッサ201と攻撃検知部202を含む。プロセッサ201は、WWWやTelnetなどのネットワークサービスを提供するプロセスを実行しながら、当該プロセスの状況を攻撃検知部202へ随時伝達する。攻撃検知部202は、プロセッサ201から入力されるプロセス状況を監視しながら、攻撃の有無を検査し、攻撃が認められた場合には攻撃内容を報告するためのアラートを生成しファイアウォール装置1へ送出する。

50 【0039】

制御インタフェース106を通してアラートを入力すると、防御ルール判定部107は、アラートの内容に従ってアクセス制御リスト管理部102のアクセス制御リストの更新等を指示する。

#### 【0040】

図3は、図2のファイアウォール装置1におけるアクセス制御リスト管理部102の模式的構成図である。アクセス制御リスト管理部102は、アクセス制御リストデータベース1021、検索部1022および更新処理部1023を有する。アクセス制御リストデータベース1021は、少なくとも「ソースIPアドレス」、「ディスティネーションIPアドレス」および「フィルタ処理方法」といったフィールドを有するエントリ（アドレス制御ルール）の集合を検索可能に保持する。検索部1022は、パケットフィルタ101からIPアドレスなどを含む問い合わせ（RQ）を受けると、アクセス制御リストデータベース1021から対応するアクセス制御ルールを検索してパケットフィルタ101へ返す。更新処理部1023は、防御ルール判定部107から入力した更新用アクセス制御ルールに従ってアクセス制御リストデータベース1021の内容を更新（追加／修正）する。

#### 【0041】

図4は、アクセス制御リストデータベース1021の内容を例示した模式図である。アクセス制御リストデータベース1021には複数のアクセス制御ルールが所定の規則に従って格納される。各アクセス制御ルールは、図4に示すように、ソースIPアドレス（SRC）やディスティネーションIPアドレス（DST）などのルール適合条件と、パケットの受理（ACCEPT）、拒否（DENY）、廃棄（DROP）などの所定の処理方法（PROC）を示す識別子との組からなる。アクセス制御ルールは一般に複数設定されるので、その集合をアクセス制御リストデータベース1021で保持しておく。図4において、アスタリスク（\*）は任意のアドレスを示し、パケットフィルタ処理の“ACCEPT”はパケットの受理、“DENY”はICMPエラー通知をするパケット拒否、“DROP”はICMPエラー通知をしないパケット廃棄をそれぞれ示す。

#### 【0042】

図5は、誘導部103に設けられた誘導リストの一例を示す模式図である。誘導部103には、予め1つ以上のIPアドレスからなる誘導リストが保持されている。本実施例の誘導リストでは、内部ネットワーク4の未使用IPアドレスが列挙されている。後述するように、未使用であるはずのIPアドレスを宛先とするパケットは、不審パケットである可能性が高い。

#### 【0043】

図6は、防御ルール判定部107に保持されている防御ルールスクリプトを例示した模式図である。詳しくは

後述するが、防御ルール判定部107は、探査（RECON）、侵入（INTRUSION）、破壊（DESTRUCTION）などの攻撃種別ごとに、防御ルールを列挙し、例えばファイル形式で保持している。防御ルールは、所定の攻撃カテゴリに1対1対応する形式で、1つのアクセス制御ルールの雛型を指定する記述が用いられる。例えば、

```
INTRUSION: (SRC: $ {SOURCE_
IP_ADDRESS}、DST: *, PROC: DR
OP)
```

といった記述が行ごとに攻撃種別ごとに列挙されている。この記述のうち「\$ {SOURCE\_IP\_ADDRESS}」の部分が、後述するように、おとり装置2からのアラートに記載された情報（攻撃パケットのソースIPアドレス）で置き換えられる変数である。

#### 【0044】

##### 1. 2) 動作

##### 1. 2. 1) パケットフィルタリング

図7は、本発明の第1実施形態による攻撃防御システムの動作を示すフローチャートである。まず、ファイアウォール装置1において、インターネット3から内部ネットワーク4へ向けたIPパケットを外部通信インタフェース100で捉えた後、当該IPパケットをパケットフィルタ101へ転送する（ステップA1）。

#### 【0045】

次に、パケットフィルタ101は、当該IPパケットのヘッダを参照し、そこに記載されているソースIPアドレスやディスティネーションIPアドレスなどの情報をアクセス制御リスト管理部102へ出力する。アクセス制御リスト管理部102は、上述したように、入力したIPアドレスを用いてアクセス制御リストデータベース1021を検索し、ヒットした最初のアクセス制御ルールをパケットフィルタ101へ返す。アクセス制御ルールを取得すると、パケットフィルタ101は、その処理方法に従って、当該IPパケットを受理または廃棄する（ステップA2）。IPパケットを受理した場合は、当該IPパケットを誘導部103へ転送し、廃棄した場合は、直ちに次のパケットの処理へと制御を移す。

#### 【0046】

アクセス制御リスト管理部102におけるアクセス制御ルールの検索において、パケットフィルタ101から入力したソースIPアドレスを検索部1022が受け取ると、検索部1022は個々のアクセス制御ルールの適合条件と入力したソースIPアドレスとを照合し、適合条件を満たす最初のアクセス制御ルールを抽出し、パケットフィルタ101へ返す。

#### 【0047】

##### 1. 2. 2) パケット誘導

次に、誘導部103では、パケットフィルタ101で受理されたIPパケットに対して、そのディスティネーションIPアドレスと予め設けられた誘導リストとを参

照し、転送すべき内部通信インタフェース（104あるいは105）を決定する（ステップA3）。具体的には、図5に示すような誘導リストと、ディステーションIPアドレスとを照合し、合致するものがある場合には、第2の内部通信インタフェース105を介して当該IP packetsをおとり装置2へ転送する。合致するものがない場合には、第1の内部通信インタフェース104を介して内部ネットワーク4へ当該IP packetsを伝達する。

#### 【0048】

IP packetsが内部ネットワーク4へ伝達された場合には、当該IP packetsは内部ネットワーク4上の適切なサーバ装置301に到達し、所定のサービスを提供するための処理が行われる（ステップA4）。

#### 【0049】

一方、IP packetsがおとり装置2へ伝達された場合には、そのプロセッサ201において、偽のサービスを提供するための処理を行いながら、入力データの内容や処理状況を逐次的に攻撃検知部202へ通知する（ステップA5）。この際、おとり装置2は、ファイアウォール装置1から伝達されたIP packetsを、そのディステーションIPアドレスの如何を問わず、受信することができる。具体的には、おとり装置2に複数のIPアドレスを割り当てられるような工夫を施してもよいし、あるいは図8に示すように、予め誘導部103にアドレス変換部1031を備えておき、入力IP packetsのディステーションIPアドレスをおとり装置2のIPアドレスに書き換えた上で、おとり装置2に当該IP packetsを伝達するような方法を用いてもよい。

#### 【0050】

##### 1. 2. 3) 偽サービス提供

IP packetsを受信後、おとり装置2は、偽のサービスとして、WWWやTelnetなど1つ以上の任意のものを提供する。ただし、本実施形態においては、通信プロトコルさえ適切に処理すれば十分であり、実際のサービスで行われるような、ファイルシステムへのアクセスやデータベース処理などは一切行わなくともよい。具体的には、例えば、Telnetサービスの場合であれば、Login/Passwordプロンプトへの任意の入力に対して、すべてログインを許可し、ユーザに偽のメッセージを応答するような偽装シェルを起動するようにしてもよい。

#### 【0051】

##### 1. 2. 4) 攻撃検知

次に、おとり装置2の攻撃検知部202では、プロセッサ201から通知される処理状況について、正常動作定義との照合を行い、攻撃の有無を判定する（ステップA6）。正常動作定義とは、おとり装置2上で提供されるサービスの正しい振舞いに関する条件の集合である。具体的には、例えば、WWWサービスに対して「WWW

サービスに対応するプロセスは自ら他のサーバ装置にネットワークアクセスをすることはしない」というような条件や、「/usr/local/www/logsディレクトリ以外にファイルを書き込むことはしない」というような条件などの集合である（詳しくは、図12参照）。これらの各条件と通知された処理状況とを照合し、合致しない条件を少なくとも1つ検出した際に、「攻撃あり」と判断する。

#### 【0052】

- 10 攻撃を検出した際、違反した条件の意味に応じて、攻撃種別を決定し、その結果をアラートとしてファイアウォール装置1へ送信する（ステップA7）。

#### 【0053】

攻撃種別とは、当該攻撃に対する防御方法を導出するのに十分な分類をいい、例えば、

- ・「探査」：ポートスキャンやバナー攻撃などのいわゆる「フィンガープリンティング」

- ・「侵入」：トロイの木馬やアカウントの追加などのバックドア設置

- 20 ・「破壊」：Ping Of Deathなどのサービス不能攻撃

などを指す。その方法の一例として、正常動作定義の中の各条件について、違反時に想定される攻撃種別を予め併記しておけばよい。例えば、前記した「/usr/local/www/logsディレクトリ以外にファイルを書き込むことはしない」という条件に違反するような攻撃については、バックドア設置の可能性が高いため、「侵入」を示す識別子を当該条件に併記しておく。

#### 【0054】

- 30 1. 2. 5) アクセス制御リストの更新

最後に、ファイアウォール装置1における防御ルール判定部107では、制御インタフェース106を介しておとり装置2から受信したアラートを参照し、防御ルールを用いてアクセス制御ルールを生成し、アクセス制御リスト管理部102へ当該アクセス制御ルールを追加するよう指示する（ステップA8）。

#### 【0055】

具体的には、防御ルール判定部107に、予め攻撃種別ごとに、図6のような防御ルールスクリプトを設定しておく。防御ルールスクリプトには、図6のような書式によって、攻撃種別と更新すべきアクセス制御ルールのひな型との組を記述する。アクセス制御ルールのひな型には、アラートに記載された情報を挿入するための変数が記述できる。たとえば、

(SRC:\$ {SOURCE\_IP\_ADDRESS}、DST:1. 2. 3. 4、PROC:DROP)と記述されている場合、「\$ {SOURCE\_IP\_ADDRESS}」の箇所は、アラートに記載されたソースIPアドレスで置換され、

(SRC:12. 34. 56. 78、DST:1.

## 2. 3. 4、PROC: DROP)

といった完全な形式のアクセス制御ルールに変換される。そして、当該アクセス制御ルールは、アクセス制御リスト管理部102内の更新処理部1023へ伝達され、アクセス制御リストデータベース1021に適切に追加される。同じソースIPアドレスおよびディステーションIPアドレスの組をもつアクセス制御ルールが既にアクセス制御リストデータベース1021に登録されている場合には、更新処理部1023は、新たに追加されたアクセス制御ルールが有効になるように適切にアクセス制御リストデータベース1021を更新する。たとえば、アクセス制御リストデータベース1021の検索スキャン方向の先頭に位置するように追加される。

## 【0056】

## 1. 3) 効果

第1実施形態のファイアウォール装置1では、誘導部103において、誘導リストとディステーションIPアドレスとの照合結果により、おとり装置2へ誘導する方法を用いている。このために、内部ネットワーク4の既存の構成を一切変更することなく、おとり装置2を設置可能となる。さらに、誘導リストに含めるIPアドレスとして、内部ネットワーク4における未使用のIPアドレス群を記載することで、1台のおとり装置2で、内部ネットワーク4上に複数のおとり装置2を設置するのと同じ効果が得られる。

## 【0057】

通常、「CodeRed」や「Nimda」などの自動感染機能をもつワームは、ある連続したIPアドレスの区間からランダムにIPアドレスを選択しながら、感染を試みるよう動作する。したがって、おとり装置2は設置台数が多ければ多いほど検知の確率が高くなる。本実施形態では、図5に示すような誘導リストの作成でその効果を得ることができる。

## 【0058】

また、ファイアウォール装置1の外部通信インタフェース100に割り当てられたIPアドレスを誘導リストに含めることで、インターネット3側からは、ファイアウォール装置1とおとり装置2との見分けがつかなくなる。一般に、インターネット3からの攻撃は、ファイアウォールの発見から始まるので、本実施形態はファイアウォール装置1を「隠す」という効果をもつ。

## 【0059】

## 1. 4) 具体例

図9～図11は第1実施形態の具体的な動作例を説明するためのネットワーク構成図であり、図12はおとり装置2における攻撃検知動作を説明するための模式図である。

## 【0060】

図9に示すように、インターネット3上に攻撃元ホスト301(IPアドレス: 12. 34. 56. 78)が

あり、内部ネットワーク4上にインターネットサーバ装置401がありものとする。さらに、インターネット3と内部ネットワーク4との境界にファイアウォール装置1が設置され、標準的なポート番号であるTCP80番ポートにおいてWWWサービスを提供するおとり装置2が設置されているものとする。また、内部ネットワーク4のネットワークアドレスとして、「1. 2. 3. x/24」が用いられており、サーバ装置401には「1. 2. 3. 4」というIPアドレスが設定されているものとする。

## 【0061】

今、攻撃元ホスト301はWWWサービスに対する自動感染機能をもつワームに感染しており、当該ワームが次の感染先として、内部ネットワーク4に対応する「1. 2. 3. x/24」に狙いを定め、かつ「1. 2. 3. 1」を第1の感染先として選択したものとする。このとき、攻撃元ホスト301から内部ネットワーク4に向けて、SYNパケット(ソースIPアドレス: 12. 34. 56. 78、ディステーションIPアドレス: 1. 2. 3. 1)が送信される。

## 【0062】

当該SYNパケットは、まず、ファイアウォール装置1の外部通信インタフェース100に到達した後、ただちにパケットフィルタ101に伝達される。パケットフィルタ101では、アクセス制御リスト管理部102に対して、少なくとも当該SYNパケットのソースIPアドレス「12. 34. 56. 78」とディステーションIPアドレス「1. 2. 3. 1」とを出力する。この他、アクセス制御ルールの粒度を高めるために、プロトコル番号「6」(TCPを示す)や、ポート番号「80」などを出力できるようにしてもよいが、本実施例では例としてソースIPアドレスとディステーションIPアドレスだけをを入力するものとする。

## 【0063】

アクセス制御リスト管理部102におけるアクセス制御リストデータベース1021は、例えば、図4のようなテキスト形式で記述されたアクセス制御リストを保持しているものとする。上述したように、各行は1つのアクセス制御ルールを示しており、SRCフィールドとDSTフィールドとの組が適合条件を、PROCフィールドがフィルタ処理方法をそれぞれ示す。

## 【0064】

検索部1022では、パケットフィルタ101から入力として与えられたソースIPアドレス「12. 34. 56. 78」およびディステーションIPアドレス「1. 2. 3. 1」との組を検索キーとして、適切なアクセス制御ルールを抽出するために、アクセス制御リストデータベースの先頭行から順に各アクセス制御ルールを参照しながら、各ルールの適合条件と前記入力との比較を行い、適合する最初のアクセス制御ルールを抽出す



る。この時点では、「(SRC:\*, DST:1. 2. 3. 1, PROC:ACCEPT)」(「PROC:ACCEPT」は入力IPパケットの受理を示す)というアクセス制御ルールが適合したとする。このとき、検索部1022は、「(SRC:12. 34. 56. 78, DST:1. 2. 3. 1, PROC:ACCEPT)」をパケットフィルタ101に返す。

#### 【0065】

アクセス制御ルールを受け取ったパケットフィルタ101は、当該ルールのPROCフィールドを参照し、「ACCEPT」であることを確認すると、ただちに入力IPパケットを後段の誘導部103へと伝達する。

#### 【0066】

続いて、誘導部103では、受け取った入力IPパケットのディスティネーションIPアドレスと内部的に保持する誘導リストとを参照し、次の転送先を決定する。本実施例では、誘導リスト内に内部ネットワーク4の未使用IPアドレスが列挙されており、その1つが「1. 2. 3. 1」であるものとする。この場合、誘導部103は、入力IPパケットのディスティネーションIPアドレス「1. 2. 3. 1」が誘導リストに記載されているのを確認した後、当該入力IPパケットをおとり装置2が接続されている第2の内部通信インタフェース105へと伝達する(図10参照)。

#### 【0067】

おとり装置2は、第2の内部通信インタフェース105へ伝達された全てのIPパケットを、そのディスティネーションIPアドレスの如何によらず受け付ける。おとり装置2では偽のWWWサービスが稼動しており、ワームが発したSYNパケットを受け付けると共に、SYN-ACKパケットをそのソースIPアドレス(すなわち攻撃元ホスト301)へ向けて出力する。

#### 【0068】

これ以降、ファイアウォール装置1で同様の処理が繰り返されて、攻撃元ホスト301とおとり装置2との間でTCP接続確立のための通信と、ワーム感染のための(不正な)通信が行われる。

#### 【0069】

おとり装置2では、プロセッサ201でWWWサービスを攻撃元ホスト301へ提供する。それと並行して、プロセッサ201は、ファイルアクセスやネットワークアクセスなどの動作状況を、攻撃検知部202へ逐次的に通知する。攻撃元ホスト301上のワームは、おとり装置2上のWWWサービスに対して、感染を試みる。具体的には、例えば、

「GET /default.ida?NNNNNNNNNNNNNNNNNNNN(200バイト程度の繰り返し)・・・%u0000%u0000=a HTTP/1.1」といった文字列から始まる、非常に大きなメッセージをWWWサービスに対して入力し、いわゆる「バッファオーバーフロ

ー」を引き起こすことで、任意のコマンドを実行しようとする。この際、一般的なワームは、ワーム自身のコードをディスク上のシステム領域にコピーした後、当該コードを実行するようなコマンドを発行する。したがって、ワームの侵入時に、プロセッサ201は、システム領域へファイルの書き出しが行われたこと、あるいは、当該ファイルの実行が行われたことを攻撃検知部202に伝達することになる。このとき、同時に、おとり装置2が受け付けた入力IPパケットのコピーも併せて伝達する。

#### 【0070】

攻撃検知部202は、予めプロセッサ201上のWWWサービスの適正な動作に関する情報を、正常動作定義ファイルとして保持している。正常動作定義ファイルは、例えば、図12のような形式で記述されており、ファイルの読み込み、書き出し、実行などに関する条件が列挙されている。

#### 【0071】

ここで、前記ワームが自身のコピーを書き出す箇所を「C:\¥Windows」ディレクトリだとすると、その動作は図12に示す正常動作定義ファイル内の第2番目の条件である

「WRITE, C:\¥Inetpub¥wwwroot¥\_vti\_log¥\*; INTRUSION」(「C:\¥Inetpub¥wwwroot¥\_vti\_logディレクトリ以下にのみファイル書き出しを行う」の意)

に違反する。このとき、攻撃検知部202は、当該条件の「;」以下を参照し、INTRUSION(侵入)カテゴリに属する攻撃があったと判定する。

#### 【0072】

続いて、攻撃検知部202は、少なくとも、入力IPパケットに含まれるソースIPアドレスと、検出された攻撃のカテゴリが「INTRUSION」であることを知らせるためのアラートを生成し、ファイアウォール装置1の制御インタフェース106へ伝達する(図11参照)。

#### 【0073】

制御インタフェース106で受信されたアラートは防御ルール判定部107へ伝達される。アラートの入力を受けた防御ルール判定部107は、上述したように、防御ルールを列挙したスクリプトを、例えばファイル形式で保持している。各防御ルールは、所定の各攻撃カテゴリに1対1対応する形式で、1つのアクセス制御ルールのひな型が指定されている(図6参照)。

#### 【0074】

具体的には、例えば、

INTRUSION: (SRC:\$ {SOURCE\_IP\_ADDRESS}, DST:\*, PROC:DROP) ... (1)



といった記述が行ごとに列挙されている。ここで、アラートの入力を受けた防御ルール判定部107は、防御ルールの定義ファイルを行ごとに参照し、「INTRUSION」カテゴリに対応する防御ルールである式(1)を抽出する。そして、アクセス制御ルールの雛型に対して、当該アラートに記載されたソースIPアドレス「12.34.56.78」(すなわち攻撃元ホストのIPアドレス)によって、「\$ {SOURCE\_IP\_ADDRESS}」を置換し、

(SRC:12.34.56.78、DST:\*, PROC:DROP) 10

... (2)

というアクセス制御ルールを生成する(「DST: \*」は任意のディステネーションIPアドレスに適合する)。そして、当該アクセス制御ルールをアクセス制御リスト管理部102へ伝達する。

【0075】

アクセス制御リスト管理部102では、防御ルール判定部107からのアクセス制御ルールの入力について更新処理部1023で処理する。更新処理部1023では、式(2)で示されるアクセス制御ルールを、アクセス制御リストデータベース1021に伝達し、その追加を指示する。アクセス制御リストデータベース1021では、式(2)で示されるアクセス制御ルールを追加するように更新処理を行う。その際、アクセス制御リストデータベース1021は、それ以降の検索処理が最近の更新結果を反映するように適切に更新処理を行う。例えば、図4のようなテキスト形式で記述されたアクセス制御リストを用い、先頭行から順に検索処理を行うような場合であれば、式(2)を先頭行に追加すればよい。つまり、たとえば式(3)といったようなアクセス制御ルールが予め設定されていたとしても、

(SRC:12.34.56.78、DST:\*, PROC:ACCEPT)

... (3)

当該更新処理以降、検索部1022がソースIPアドレス「12.34.56.78」を含む入力を受けた場合には、式(3)ではなく式(2)を検索結果として出力する(図13参照)。

【0076】

次に、攻撃元ホスト301上のワームが次の攻撃先として、「1.2.3.4」を選択したものとする。しかる後、先の攻撃と同様に、内部ネットワーク4上のサーバ装置401に向けたSYNパケットがファイアウォール装置1に到達する。その場合、当該SYNパケットの入力をうけたパケットフィルタ101は、アクセス制御リスト管理部102から適合するアクセス制御ルールとして式(2)を受け取るので、PROCフィールドの指

定「DROP」に従い、当該SYNパケットを廃棄する(図14参照)。

【0077】

以上のような動作を行うことにより、本発明による攻撃防御システムは、攻撃元ホスト301上のワームからの攻撃から、内部ネットワーク4上のサーバ装置401を保護することができる。

【0078】

(第2実施形態)

2.1) 構成

図15は、本発明の第2実施形態による攻撃防御システムのブロック図である。本実施形態のファイアウォール装置5は、図2に示す第1実施形態におけるファイアウォール装置1に信頼度管理部502を加え、さらに誘導部103に代えて、信頼度に依存してパケット誘導方向を決定できる誘導部501を有する。以下、図2に示すシステムと同じ機能ブロックについては、同一参照番号を付して詳細な説明は省略する。

【0079】

図15において、誘導部501は、パケットを入力すると、信頼度管理部502へ入力IPパケットのソースIPアドレスを出力し、対応する信頼度を取得する。信頼度を受け取ると、誘導部501はその信頼度と所定のしきい値との比較を行い、その結果に応じて、当該入力IPパケットを第1の内部通信インタフェース104および第2の内部通信インタフェース105のいずれかに出力する。

【0080】

信頼度管理部502はIPアドレスと対応する信頼度との組の集合を管理する。誘導部501から要求があると、信頼度管理部502はそれに対応した信頼度を検索して誘導部501へ返し、後述するように信頼度の更新を行う。

【0081】

2.2) 動作

図16は、本発明の第2実施形態による攻撃防御システムの動作を示すフローチャートである。

【0082】

まず、第1実施形態のファイアウォール装置1と同様に、インターネット3からの入力IPパケットを受信すると(ステップA1)、パケットフィルタ101は、アクセス制御リスト管理部102で保持されているアクセス制御ルールの内容に応じて、当該入力IPパケットの受理または廃棄を行う(ステップA2)。受理されたIPパケットは誘導部501へ転送される。

【0083】

2.2.1) 信頼度管理

誘導部501は、入力IPパケットに含まれる情報のうち少なくともソースIPアドレスを信頼度管理部502へ出力し、当該IPアドレスに対する信頼度を取得す

る(ステップC1)。信頼度管理部502はIPアドレスとその信頼度との組の集合を保持し、IPアドレスを入力すると、それに対応する信頼度を出力することができる。具体的には、例えば、「1. 2. 3. 4:10」などのように、「<IPアドレス>:<信頼度>」といった形式をなす行で構成されるテキストファイルを用いることができる。

#### 【0084】

その他、検索および更新処理を効率的に行うために、リレーショナルデータベースを利用してもよい。いずれにせよ、任意のIPアドレスについて、対応する信頼度を適切に検索および更新できればよい。信頼度管理部502は、入力されたIPアドレスに対応するIPアドレスと信頼度との組が1つ見つければ、当該信頼度を誘導部501へ出力する。もし適切なIPアドレスと信頼度の組が見つからなかった場合には、当該IPアドレスに対する信頼度として初期値(例えば0)を設定し、当該初期値を誘導部501に出力するとともに、新たに「<IPアドレス>:<初期値>」という組を保持内容に追加する。

#### 【0085】

続いて、信頼度管理部502は、信頼度を出力した後、当該信頼度を増加させるように保持内容を更新する(ステップC2)。具体的には、例えば次式(4)に示されるように、信頼度に定数C( $\geq 1$ )を加算する。

#### 【0086】

$$c[n+1] = c[n] + C \quad \dots (4)$$

#### 【0087】

##### 2. 2. 2) 信頼度に基づくパケット誘導

誘導部501は、取得した信頼度に応じて、当該IPパケットの転送先を決定する(ステップC3)。信頼度cの評価処理の好適な一例としては、予め誘導部501にあるしきい値Tを設定しておき、信頼度cとしきい値Tとの比較結果(大小関係)を評価する。

#### 【0088】

図17は、本実施形態における信頼度とパケット転送先の関係を示すグラフである。ここでは、 $c \geq T$ のときには、入力IPパケットを「信頼できる」と判定し、当該IPパケットを内部通信インタフェース104を介して内部ネットワーク4へ伝達する。一方、 $c < T$ のときには、内部通信インタフェース105を介して、おとり装置2へ伝達する。

#### 【0089】

なお、これ以降の動作は、図7に示す処理(ステップA4~A8)と同じである。

#### 【0090】

##### 2. 2. 3) 信頼度の更新方法

図16のステップC2における信頼度の更新方法は、上述した式(4)の他に、別の方法もある。次式(5)に示すように、誘導部501からの入力の一部に、入力

IPパケットpのバイト数L(p)を含めておき、その逆数 $1/L(p)$ を加算するようにしても良い。

#### 【0091】

$$c[n+1] = c[n] + 1/L(p) \quad \dots$$

#### (5)。

#### 【0092】

この方法は、大きなサイズをもつIPパケットほど信頼度が増加しにくくなるように、重みづけを行うものである。一般に、バッファオーバーフロー攻撃やサービス妨害(DoS)攻撃を目的としたIPパケットは正常な通信内容をもつIPパケットに比べて大きなサイズをもつことが多いため、こうした重みづけを施すことで、これらの攻撃の可能性をもつ入力IPパケットを、できるだけ長い期間、おとり装置2へ誘導することが可能になる。その結果、本発明による攻撃防御システムの防御性能を高めることができる。

#### 【0093】

また、別の一例として、誘導部501からの入力の一部に、入力IPパケットのプロトコル番号を含めておき、予め設定されたプロトコル番号に一致した場合のみ、信頼度を更新する方法を併用してもよい。たとえば、予めプロトコル番号「6」を設定しておくことで、入力IPパケットがTCPである場合にのみ、信頼度を更新する。こうすることで、本格的な攻撃の前に準備的に行われるスキャン攻撃による、不要な信頼度の増加を抑える効果が得られる。もちろん、更新処理の条件として、プロトコル番号だけでなく、その他IPヘッダ、TCPヘッダ、UDPヘッダなどに含まれる任意の情報を利用してもよいし、複数の条件を組み合わせた論理式を用いるようにしてもよい。

#### 【0094】

さらに別の一例として、入力IPパケットについて、一般に外れ値検知として知られるような、統計的に「異常であること」の確からしさを求める方法を用いてもよい。具体的には、図18に示すように、IPアドレスと信頼度との組の集合に代えて、特開2001-101154公報(本出願人による特許出願)に記載の外れ値度計算装置を信頼度管理部502に組み込む。この場合、誘導部501からは実数値や属性を表す離散値などを含む多次元のベクトル、たとえば、 $x = (\text{入力IPパケットの到達時刻}, \text{入力IPパケットのサイズ}, \text{プロトコル番号})$ を入力する。

#### 【0095】

このような多次元ベクトルを入力した外れ値度計算装置は、それまでの入力から生成した確率密度分布などを基に、1個の実数値として表される「スコア値」を算出する。このスコア値は「異常であること」の確からしさを表しており、その値が大きいほど攻撃である可能性が高い、言い換えれば信頼度が低い。したがって、スコア値の逆数をもって、入力IPパケットに対する信頼度と

することができる。

#### 【0096】

図18(A)は、外れ値度計算を用いた信頼度管理部502の概略的構成図であり、(B)は、その一例を示す詳細なブロック図である。この外れ値度計算を用いる方法は、上述したような「決定的な」信頼度の評価方法では捉えきれない(すなわち予測されない)攻撃を「確率的に」検出するものである。したがって、将来現れる未知の攻撃に対する防御が可能となる。

#### 【0097】

本発明の第2実施形態は、第1実施形態による効果に加えて、さらに「アクティブ・ターゲティング」にも対応できるという効果が得られる。アクティブ・ターゲティングとは、次に具体的に説明するように、予め特定のサーバ装置もしくはホスト装置に狙いを定めて行われる攻撃形態を指し、一般的には悪意をもった人間によって実行される。

#### 【0098】

##### 2. 3) 具体例

図19～図21は、本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

#### 【0099】

図19に示すように、インターネット3上の攻撃元ホスト301を使うユーザが、内部ネットワーク4上のサーバ装置401の動作停止を目的として、Ping of DeathなどのDoS攻撃を行う場合を考える。

#### 【0100】

このような場合、攻撃元ホスト301のIPアドレス「12.34.56.78」に対する信頼度が、誘導部501に設定されたしきい値以下であれば、図20に示すように、DoS攻撃を構成するIPパケットはおとり装置2へ誘導され、サーバ装置401は保護される。DoS攻撃をしかけるような悪意をもった人間は、ターゲットを定めたとばかり後に、攻撃を開始すると考えられるので、前記しきい値を十分大きく設定しておくことで、おとり装置2によるサーバ装置401の保護が達成される。

#### 【0101】

さらに、通常の(すなわち攻撃の意図がない)ユーザからのアクセスについては、安全に内部ネットワーク4上のサーバ装置401によるサービスを行うことができる。たとえば、図21に示すように、インターネット3上に通常のホスト302から、サーバ装置401へのアクセスがあった場合、前記例と同様に、ファイアウォール装置5の信頼度管理部502により、通常のホスト302のIPアドレスに対する信頼度が評価される。

#### 【0102】

もし、通常のホスト302の信頼度が不十分であれば、誘導部501により「不審」と判定され、おとり装

置2へ当該アクセスを構成するIPパケットは誘導される。ここで、おとり装置2のプロセッサ201で、サーバ装置401上のWWWサービスと同じ処理を行うよう、おとり装置2を設定しておく。すなわち、おとり装置2をサーバ装置401のミラーサーバとして動作させる。具体的には、WWWサービスの場合、HTMLファイルやJPEGファイルなどのコンテンツの複製をとればよい。したがって、通常のホスト302は目的のサービスを受けることができる。おとり装置2では正常なアクセスがなされる間は攻撃が検知されることがないので、通常のホスト302のIPアドレスに対する信頼度は上述した信頼度更新方法に従って増加していき、いずれ、しきい値Tを超える。信頼度cがしきい値Tを超えた後は、通常のホスト302からのアクセスを構成するIPパケットは内部ネットワーク4内のサーバ装置401へ誘導される。

#### 【0103】

このような動作により、信頼ずみの通常のユーザからのアクセスについては、すべてサーバ装置401が応答する。したがって、おとり装置2が攻撃を受けて、その動作を停止したとしても、信頼ずみの通常のユーザは、サーバ装置401によりサービスを継続して受けることができるという効果をもつ。

#### 【0104】

なお、おとり装置2はサーバ装置401上の完全なミラーサーバとして設定してもよいし、例えば、ユーザ認証を要するような重要サービスは除いて、一般的なサービスだけをおとり装置2で提供するようにも設定できる。

#### 【0105】

##### (第3実施形態)

図22は、本発明の第3実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図であり、図23は、その一例を示す詳細なブロック図である。本実施形態のファイアウォール装置6は、ファイアウォール装置1における誘導部103に加えて、図5に示す第2実施形態の誘導部501および信頼度管理部502を有する。

#### 【0106】

具体的には、図23に示すように、第1の誘導部103の後段として第2の誘導部501を設けても良い。逆に、第1の誘導部103の前段として第2の誘導部501を設けることもできる。

#### 【0107】

いずれの構成においても、ワームのようにランダムにIPアドレスを選択して行われる攻撃と、アクティブ・ターゲティングによる攻撃の両方に対応できる、という効果が得られる。また、あるホストが、第2の誘導部501で一旦信頼された後、ワームに感染するなどした場合でも、おとり装置2にて攻撃の有無を検査すること

ができる、という効果も得られる。

#### 【0108】

##### (第4実施形態)

##### 4. 1) 構成

図24は、本発明における第4実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。本実施形態によるファイアウォール装置7は、図15のファイアウォール装置5における信頼度管理部502に代えて、信頼度管理部701が接続されている。その他の機能ブロックは、図15のものと同じであるから、同一参照番号を付して説明は省略する。

#### 【0109】

図24に示すように、信頼度管理部701は、リアルタイム信頼度データベース7011、複製処理部7012、長期信頼度データベース7013、および、更新処理部7014を備える。

#### 【0110】

リアルタイム信頼度データベース7011は、IPアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理し、誘導部501からの問い合わせのIPアドレスに応じて、対応する信頼度を返す。複製処理部7012は、定期的に、リアルタイム信頼度データベース7011の内容を、長期信頼度データベース7013へ複製する。

#### 【0111】

長期信頼度データベース7013は、IPアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理する。更新処理部7014は、定期的に長期信頼度データベース7013を参照し、所定の期間よりも古い最終更新時刻を有する項目について、その信頼度を減算する更新処理を実行する。

#### 【0112】

##### 4. 2) 信頼度管理

基本的には、入力IPパケットをフィルタリングし、おとり装置2または内部ネットワーク3へ誘導するまでの処理は、第2実施形態のファイアウォール装置5と同一である(図16のステップA1~A2、C1~C3、A4~A8)。ただし、本実施形態の信頼度管理部701は、パケットの処理と並行して、以下にあげるような信頼度管理処理を行う。

#### 【0113】

図25は信頼度管理部701における信頼度参照処理を示すフローチャートである。まず、図16のステップC1において信頼度の参照が行われたとき、信頼度管理部701は、リアルタイム信頼度データベース7011から、入力として与えられたIPアドレスに対応する項目が記録されているかどうかを調べる(図25のステップD1)。当該IPアドレスに対応する項目が記録されている場合(ステップD1のY)、さらにその信頼度を参照し、当該信頼度を誘導部501に出力する(ステッ

プD2)。

#### 【0114】

一方、IPアドレスに対応する項目がリアルタイム信頼度データベース7011に記録されていない場合(ステップD1のN)、まず、長期信頼度データベース7013を参照して、当該IPアドレスに対応する項目が記録されているかどうかを調べる(ステップD3)。記録されている場合(ステップD3のY)、長期信頼度データベース7013の該当項目の内容(IPアドレス、信頼度および最終更新時刻)を、リアルタイム信頼度データベース7011にコピーし(ステップD4)、信頼度を出力する(ステップD2)。長期信頼度データベース7013にも該当項目がない場合(ステップD3のN)、リアルタイム信頼度データベース7011に、所定の信頼度の初期値をもって、新たな項目を追加し(ステップD5)、信頼度を出力する(ステップD2)。

#### 【0115】

そして、図16のステップC2において信頼度の更新が行われたとき、信頼度管理部701は、IPアドレスと、信頼度の更新に加えて、更新時刻をリアルタイム信頼度データベース7011に記録する。

#### 【0116】

##### 4. 3) リアルタイム信頼度の複製処理

以上の処理と並行して、複製処理部7012は定期的に(例えば1日ごとに)リアルタイム信頼度データベース7011の全内容を走査しながら、各項目を長期信頼度データベース7013へコピーしていく。このとき、最終更新時刻を参照して、所定の期間(例えば1週間)以上、更新処理が行われなかった項目について、当該項目をリアルタイム信頼度データベース7011から削除する処理を行っても良い。

#### 【0117】

##### 4. 4) 長期信頼度の更新処理

また、更新処理部7014は、定期的に(例えば1日ごとに)長期信頼度データベース7013の全内容を走査しながら、各項目の最終更新時刻を参照して、所定の期間(例えば1週間)以上、更新が行われなかった項目については、その信頼度を所定の値だけ減算する。もしくは、単に削除しても良い。

#### 【0118】

##### 4. 5) 効果

以上のような動作を行うことで、リアルタイム信頼度データベース7011の記憶容量を抑えることができるので、SDRAMなど、低容量で高速な記憶デバイスを用いることができる。一方、長期信頼度データベース7013はアクセス頻度が少ないので、ハードディスクデバイスなど、大容量で低速な記憶デバイスを用いることができる。

#### 【0119】

また、更新処理部7014による長期信頼度データベ

ース7013の更新処理により、たとえ1度、十分な信頼度を得たソースIPアドレスについても、ある一定期間以上、アクセスが途絶えた場合には再び「不審」と見なすことができる。これは、特に中古PCの売買など、ソースIPアドレスに相当するホストの利用環境が大きく変化した場合などに、信頼度の再評価を自動的に起こすことができるという効果をもつ。

#### 【0120】

##### (第5実施形態)

本発明の第5実施形態として、図23に示す第3実施形態の信頼度管理部502に代えて、上述した第4実施形態の信頼度管理部701を用いたファイアウォール装置を構成することができる。基本的な構成は図23と同じであり、信頼度管理部701の構成及び動作は、図24、図25および第4実施形態の項で説明した通りであるから、ここでは省略する。

#### 【0121】

##### (第6実施形態)

##### 6. 1) 構成

図26は、本発明の第6実施形態による攻撃防御システムのファイアウォール装置9を示す概略的ブロック図である。ファイアウォール装置9では、第1実施形態のファイアウォール装置1における誘導部103に代えて、バッファ9011およびICMP監視部9012を有する誘導部901が設けられている。本実施形態では、第1実施形態のように誘導リストを設けることなく、ICMPパケットを利用して同様の機能を実現できる。なお、簡略化のために、図26では他の機能ブロックの表示が省略されている。

#### 【0122】

バッファ9011は、次に述べるように、パケットフィルタ101より受け取ったパケットを一時的に蓄積し、第1内部通信インタフェース105を介して内部ネットワークへ転送すると共に、ICMP監視部9012からの求めに応じて、蓄積したパケットを第2の内部通信インタフェース105を介しておとり装置2へ再送信する。ICMP監視部9012は、第1の内部通信インタフェース104におけるICMPパケットの受信を監視し、特定のICMPエラーパケットを検出したとき、バッファ9011に適切なパケット再送を要求する。以下、本実施形態の動作を詳述する。

#### 【0123】

##### 6. 2) 動作

図27は本実施形態によるファイアウォール装置9の動作を示すフローチャートである。まず、第1実施形態のファイアウォール装置1と同様に、外部通信インタフェース100を介してインターネット4から受信した入力IPパケットについて、パケットフィルタ101によるフィルタリングを行う(ステップA1、A2)。

#### 【0124】

受理されたIPパケットは誘導部901のバッファ9011に蓄積され(ステップE1)、無条件に第1の内部通信インタフェース104を介して内部ネットワーク3へ送出され(ステップE2)、通常のサービスが提供される(ステップA4)。この場合、たとえ不審パケットであっても内部ネットワークへ転送されてしまうが、実際の攻撃を実行する前に送信されるTCPコネクション確立要求のSYNパケットは攻撃要素が含まれていないために、SYNパケットであれば受け入れても問題はない。内部ネットワークにSYNパケットが転送され宛先が存在しなければ、到達不能を知らせるICMPパケット(タイプ3)が返される。

#### 【0125】

ICMP監視部9012は、第1の内部通信インタフェース104でICMPパケット(RFC792記載)が受信されると、当該ICMPパケットの内容を参照して、到達不能を知らせるエラー(すなわちICMPタイプ3)であるか否かを調べる(ステップE3)。到達不能を知らせるエラーであれば(ステップE3のY)、そのIPヘッダ部をさらに参照し、少なくともソースIPアドレスもしくはディスティネーションIPアドレスを用いてバッファ9011に再送要求を行う(ステップE3)。その他のメッセージであった場合は、何もせず、監視を続ける。

#### 【0126】

再送要求を受けたバッファ9011は、少なくともソースIPアドレスもしくはディスティネーションIPアドレスに従って、蓄積されたパケットから該当するパケットを抽出し、当該パケットを第2の内部通信インタフェース105を介して、おとり装置2へ再送する(ステップE4)。以下、すでに述べたステップA5~A8が実行される。

#### 【0127】

このように攻撃要素を含まないコネクション確立のためのパケットを利用することで、内部ネットワーク3の未使用IPアドレスを誘導リストとして事前に設定することなしに、自動的に未使用IPアドレス宛ての入力IPパケットをおとり装置2へ誘導することができる。

#### 【0128】

##### (第7実施形態)

##### 7. 1) 構成

図28は、本発明の第7実施形態による攻撃防御システムのファイアウォール装置10を示す概略的ブロック図である。このファイアウォール装置10は、上述した第2~第5実施形態によるファイアウォール装置における防御ルール判定部107およびアクセス制御リスト管理部102に代えて、有効期限付き防御ルール判定部1001および有効期限付きアクセス制御リスト管理部1002を設けている。

#### 【0129】

防御ルール判定部1001は、制御インタフェース106を介しておとり装置2から受け取ったアラートに応じて、信頼度管理部502および701に対して、対応する信頼度の再設定を指示する。あるいは、アラートに応じて、更新すべきアクセス制御ルールを決定し、アクセス制御リスト管理部1002にその更新を指示する。

#### 【0130】

信頼度管理部502および701は、防御ルール判定部1001からの更新指示を受けて、新たな信頼度を決定し誘導部501へ出力する。アクセス制御リスト管理部1002は、防御ルール判定部1001からの更新指示を受けて、アクセス制御リストを更新し、パケットフィルタ101からの要求に応じてアクセス制御ルールを出力する。

#### 【0131】

##### 7. 2) 動作

本実施形態における攻撃防御システムの動作を、具体的な例を挙げながら詳細に説明する。

#### 【0132】

まず、インターネット4から到達した入力IPパケットが、ファイアウォール装置10によって、おとり装置2へ誘導され、おとり装置2において、当該入力IPパケットによる攻撃が検知され、その旨を知らせるアラートが送信されるまでは、図16のステップA1～A7に示すように、第2～第5実施形態における攻撃防御システムと同様である。

#### 【0133】

ファイアウォール装置10の防御ルール判定部1001には、防御ルール判定部107とは異なり、信頼度を更新するための防御ルールが予め設定されている。例えば、防御ルールとして、次式(6)のような形式の記述があれば、信頼度を1減算すると解釈されるものとす

#### 【0134】

RECON: c (\$ {SOURCE\_\_IP\_\_ADDRESS}) - = 1

... (6)。

#### 【0135】

たとえば、制御インタフェース106を通してソースIPアドレス「12. 34. 56. 78」を示すアラートが受け取ると、防御ルール判定部1001はIPアドレス「12. 34. 56. 78」に対する信頼度を1減算すると解釈し、その旨を信頼度管理部502/701に指示する。すなわち、アラートを受け取ると、そのソースIPアドレスの信頼度を低減させる。信頼度管理部502は第2実施形態で説明したように信頼度を更新し、信頼度管理部701は第4実施形態で説明したように信頼度を更新するから、信頼度の低減処理を加えることで、よりきめ細かい信頼度管理ができる。

#### 【0136】

また、ファイアウォール装置10において、防御ルール判定部1001内に、防御ルール判定部107と同様に、アクセス制御ルールのひな型としての防御ルールを予め設定してもよい。ただし、この場合のアクセス制御ルールは、新たに「有効期間」を表すフィールドを記載できる(したがって防御ルールにも記載可能)。例えば、次式(7)に示すように、前記式(1)の防御ルールにEXPIREの項を追加し、「7日間有効」という制約をつけることができる。

#### 【0137】

INTRUSION: (SRC: \$ {SOURCE\_\_IP\_\_ADDRESS}, DST: \*, PROC: DROP, EXPIRE: +7DAY) ... (7)。

#### 【0138】

したがって、アラートが制御インタフェース106を経由して防御ルール判定部1001に伝達されると、防御ルール判定部107と同様の方法で、次式(8)に示すようにアクセス制御ルールが生成され、アクセス制御リスト管理部1002に伝達される。

#### 【0139】

(SRC: 12. 34. 56. 78, DST: \*, PROC: DROP, EXPIRE: +7DAY) ... (8)。

#### 【0140】

次に、アクセス制御リスト管理部1002は、防御ルール判定部1001から受け取ったアクセス制御ルールをアクセス制御リストデータベース1021に追加する。このとき、式(8)のようにEXPIREフィールドがアクセス制御ルールに記載されている場合、アクセス制御リスト管理部1002は、現在時刻に、EXPIREフィールドに指定された値を加算した時刻を算出した上で、データベースを更新する(図7のステップA8に対応する)。

#### 【0141】

図29は、アクセス制御リスト管理部1002の管理動作を示すフローチャートである。アクセス制御リストデータベース1021が更新された後、再びソースアドレス「12. 34. 56. 78」からの入力IPパケットがファイアウォール装置10に到達すると、パケットフィルタ101は当該ソースIPアドレスをアクセス制御リスト管理部1002へ送付してアクセス制御ルールの取得要求を行う(ステップA2\_1)。

#### 【0142】

アクセス制御リスト管理部1002は、当該ソースIPアドレスに対応するアクセス制御ルールを検索する(ステップA2\_2、A2\_3)。式(8)に相当するアクセス制御ルールを抽出すると、アクセス制御リスト管理部1002は、EXPIREフィールドに記載された有効期間と現在時刻とを比較する(ステップA2\_

4)。

#### 【0143】

現在時刻が有効期間を超過していた場合には(ステップA2\_4のYES)、当該アクセス制御ルールをアクセス制御リストデータベース1021から削除し(ステップA2\_5)、デフォルトのアクセス制御ルールをパケットフィルタ101へ返す(ステップA2\_6)。逆に、有効期間内であれば(ステップA2\_4のNO)、次式(9)に示すようなEXPIREフィールドを除いたアクセス制御ルールをパケットフィルタ101へ返す(ステップA2\_7)。

#### 【0144】

(SRC:12.34.56.78、DST:＊、PROG:DROP)

... (9)。

#### 【0145】

こうして取得したアクセス制御ルールを用いて、パケットフィルタ101は受信IPパケットの受理/廃棄の判定を行う(ステップA2)。

#### 【0146】

上述したように、攻撃をおとり装置で検知した後の防御方法として、よりきめ細かな対策を講じることができる。具体例を挙げると、一般に攻撃者は、「侵入」もしくは「破壊」に相当する攻撃の準備として、ポートスキャンあるいはTracerouteなどの「探査」に相当する攻撃を行う。しかし、「探査」として検出されるアクセスが、全て攻撃であるとは限らないことも、よく知られる所である。したがって、「探査」に対する防御方法として、恒久的なアクセス遮断を行うことは不都合を生じる可能性がある。

#### 【0147】

そこで、本実施形態では、有効期限付きのアクセス制御ルールを用いて時間制限を付けたアクセス遮断を行う。または、上述したように、アラーム発生によってそれまで蓄積された信頼度を低減させることで、信頼度がしきい値T(図17参照)を超えないようにし、おとり装置への誘導を継続し、後で「侵入」もしくは「破壊」に相当する攻撃を検知してから恒久的なアクセス遮断へと対応を変えることもできる。

#### 【0148】

##### (第8実施形態)

図30は、本発明の第8実施形態による攻撃防御システムの概略的構成図である。第8実施形態では、単一のおとり装置2に代えて、2台以上のおとり装置2を含むおとりクラスタ21が設けられている。

#### 【0149】

本実施形態における各おとり装置2は、特定のディシェンションIPアドレスをもつパケット、もしくは、特定のポート番号をもつパケットにしか偽のサービ

スを提供しないようにする。

#### 【0150】

こうすることにより、内部ネットワーク4上の特定のサーバ装置に1対1対応するおとり装置2を設けたり、特定の偽のサービスだけを提供するおとり装置2を設けたりすることができる。したがって、攻撃者に対して正規のサーバ装置により近いサービスを提供することができ、また、特定のサービス向けの正常動作定義をもつことでより運用性を向上させることもできる。

#### 【0151】

##### (第9実施形態)

第9実施形態のファイアウォール装置は、第1～第8実施形態における誘導部に加えて、出力パケット誘導部を有する。出力パケット誘導部は、内部ネットワーク3からインターネット4へ向けて送信される出力IPパケットに対して、上述したパケットフィルタリングおよびおとり装置への誘導処理を行う。

#### 【0152】

このような出力パケット誘導部を設けることで、内部ネットワーク3の運用規定として、インターネット4へのアクセスを禁じているような場合に、内部ネットワーク3からインターネット4への不法なアクセスを検知し、その記録をとることができる。

#### 【0153】

##### (第10実施形態)

上記第1～第9実施形態の説明では機能ブロック構成を用いたが、本発明はこれに限定されるものではなく、ソフトウェアにより同一の機能を実現することもできる。

#### 【0154】

図31は、本発明の第10実施形態による攻撃防御システムの概略的構成図である。本実施形態のファイアウォール装置には、プログラム制御プロセッサ1101、上記第1～第9実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ1102、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース1103、および各種インタフェース100、104～106が設けられている。同様に、本実施形態のおとり装置には、プログラム制御プロセッサ2101、上記第1実施形態で説明したおとり装置としての機能ブロックを実現するプログラムのセットを格納したプログラムメモリ2102およびファイアウォール装置とのインタフェースが設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第1～第9実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。

#### 【0155】

##### (第11実施形態)



上記第1～第10実施形態では、ファイアウォール装置とおとり装置とが別ユニットになった攻撃防御システムを例示したが、本発明はこれに限定されるものではなく、ハードウェア的に1ユニットで構成することもできる。1ユニットは、取り扱いが容易であり小型化し易いというメリットがある。

#### 【0156】

図32は、本発明の第11実施形態による攻撃防御ユニットの概略的構成図である。本実施形態の攻撃防御ユニットには、ファイアウォール装置用のプログラム制御プロセッサ1101、おとり装置用のプログラム制御プロセッサ2101、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース1103、上記第1～第9実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ1104、および各種インタフェース100および104が設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第1～第9実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。また、プロセッサ1101とプロセッサ2101とを単一のプロセッサで構成しても良い。

#### 【0157】

##### (第12実施形態)

##### 12.1) 構成

図33は、本発明の第12実施形態によるおとり装置のブロック図である。本実施形態におけるおとり装置37は、第1～第10実施形態におけるおとり装置2の攻撃検知部202に代えて、イベント管理部3701および攻撃検知部3702を備える。

#### 【0158】

イベント管理部3701は、プロセッサ201から伝達されるプロセス状況（以下イベント）を内部的に備えたキューに一時格納しながら、所定の条件を満たす関係をもつ過去のイベントとの間にリンク付けを行い、当該イベントとリンクを攻撃検知部3702に伝達する。また、攻撃検知部3702からリンクの入力を受けて、リンク先またはリンク元イベントを返す。

#### 【0159】

攻撃検知部3702は、イベントとリンクの組の伝達を受けて、必要に応じて、イベント管理部3701を用いてリンクを探索しながら、所定の攻撃検知ルールとの照合によって攻撃の有無を判定し、攻撃があった場合にファイアウォール装置にその旨を通知するためのアラームを送信する。

#### 【0160】

##### 12.2) 動作

図34は、本発明の第12実施形態によるおとり装置37の動作を示すフローチャートである。

#### 【0161】

##### 12.2.1) イベント伝達

まず、ファイアウォール装置1から転送された入力IPパケットを受けて、プロセッサ201上の偽サービスを提供するためのプログラムが動作する。第1～第10実施形態におけるおとり装置2とは異なり、この偽サービス提供は正規のサービス提供と全く同じように、ネットワーク入出力・プロセスの生成と停止（プロセス生滅）・ファイル入出力を行うものとする。

#### 【0162】

プロセッサ201は、当該プログラムを動作させながら、さらに、ネットワーク入出力・プロセス生滅・ファイル入出力に係るイベントを、イベント管理部3701に随時伝達する（ステップF1）。

#### 【0163】

イベントには、少なくとも、イベント名および引数の値や、イベントの返値や、当該イベントを発行したプロセスのプロセスIDが含まれる。この他、イベントの発生時刻などを含めてもよい。

#### 【0164】

##### 12.2.2) イベント種別の判定

イベントの伝達を受けたイベント管理部3701では、まず所定のイベント種別判定ルールに従って、イベント種別を判定する（ステップF2）。イベント種別判定ルールは、少なくともネットワーク入出力・プロセス生滅・ファイル入出力を区別できれば十分である。たとえば、プロセッサ201が伝達するイベントの名前と、イベント種別との対応関係を定めたテーブル（図35参照）を予め用意しておき、イベントが伝達されるたびに当該テーブルを検索して、イベント種別を導けばよい。

#### 【0165】

##### 12.2.3) イベント管理キューへの追加

そして、イベント管理部3701は、前記イベントをキューに格納する（ステップF3）。キューは1本でもよいが、並列処理や後段の処理を簡単にするために、複数本を備えてもよい。ここでは、たとえば、イベント種別ごとに1本ずつのキューを備えるものとする（図36参照）。この場合、前記イベント種別判定ルールによって求められたイベント種別について、対応するキューを選択し、その最後尾に前記イベントを追加する。

#### 【0166】

##### 12.2.4) イベント間のリンク付け

さらに、イベント管理部3701は、最後にキューに追加したイベント（カレントイベント）について、所定のリンク付けルールにしたがって、関連イベントとの間にリンク付けを行う（ステップF4）。リンク付けルールは、少なくともイベントの発生源となったプロセスの生成イベントから、当該イベントへのリンクを生成できれば十分である（図43参照）。関連イベントとのリンク付けを入力した攻撃検知部3702は、DT定義にしたがって攻撃の有無を判定する（ステップF5～F



7)。詳しくは後述するが、関連イベントとのリンク付けとDT定義に記載された各ルールとの照合を行い、合致するルールがあるか否かを判定し(ステップF6)、合致するルールがあれば(ステップF5のY)、さらに攻撃であるかどうかを判定する(ステップF7)。攻撃があれば、ただちにアラームを生成し、ファイアウォール装置1に送信する(ステップF8)。以下、さらに詳細に説明する。

#### 【0167】

12. 2. 4. 1) 基本的なリンク付けルール

図37を参照しながら、より具体的な例として、もっとも基本的なリンク付けルールを示す。

#### 【0168】

図37において、まず、前記カレントイベントの発行源プロセスIDを抽出する(ステップH1)。そして、プロセスイベント管理キューの最後尾にあるイベントを参照する(ステップH2)。

#### 【0169】

次に、現在参照しているイベントが、プロセス生成イベントか否かを判別する(ステップH3)。具体的には、例えば、予め定めたイベント名と、現在参照中のイベントに記載されたイベント名が一致するかどうかを検査する。

#### 【0170】

そして、プロセス生成イベントではないと判定された場合は、参照先を1つ前方に移動させ、ステップH3へ戻る(ステップH4)。

#### 【0171】

一方、プロセス生成イベントであると判定された場合は、現在参照しているイベントのプロセスIDを参照して、前記発行源プロセスIDと比較する(ステップH5)。一致する場合は、ステップH6に進み、一致しない場合は、ステップH4に戻る。

#### 【0172】

なお、カレントイベントがプロセス生成イベントである場合、ステップH2で参照されるイベントはカレントイベント自身である。しかし、どのオペレーティングシステムにおいても、プロセス生成の際に、同じプロセスIDが割り当てられることはあり得ない。したがって、ステップH5において、カレントイベントの発行源プロセスIDと、カレントイベントのプロセスIDは一致せず、必ずステップH4へ戻る。

#### 【0173】

そして、当該プロセス生成イベントから、カレントイベントへの、順方向リンクをプロセス生成イベントに付加する(ステップH6)。さらに、カレントイベントからプロセス生成イベントへの、逆方向リンクをカレントイベントに付加する(ステップH7)。順方向および逆方向のリンクの一例は図43に示される。

#### 【0174】

こうして付加された順方向リンクは、イベント間の関係を時系列に沿った形で保持するためのものであり、逆方向リンクは、イベント間の関係を時系列とは逆順に保持するためのものである。以降の処理において、イベント間の時間的な関係を利用するので、同じイベントに付加された、順方向リンクと逆方向リンクはいつでも区別できるようにしておくことが望ましい。

#### 【0175】

12. 2. 4. 2) イベントーコンテキスト対の伝達

その後、イベント管理部3701は、前記カレントイベントと、そのコンテキストとの組(イベントーコンテキスト対)を攻撃検知部3702へ出力する。図38に示すように、コンテキストとは、カレントイベントに付加された全ての順方向リンクおよび逆方向リンクの集合を指す。

#### 【0176】

12. 2. 5) 攻撃検知

図39に、予め定められたドメインータイプ制約付きの正常動作定義(以下、DT定義という。)の一例を示す。イベントーコンテキスト対の入力を受けた攻撃検知部3702は、DT定義にしたがって攻撃の有無を判定する(図34のステップF5)。

#### 【0177】

12. 2. 5. 1) ドメインータイプ制約つきルールの判定

(ドメインータイプ制約つきルールの構成要素)

DT定義内の各ドメインータイプ制約つきルールは、少なくとも、

(1) ドメインータイプ制約(以下、DT制約)

(2) イベント制約

(3) 判定値

という構成要素をもつ。

#### 【0178】

(1) DT制約は、イベントの発生原因となったアクセスの送信元ホストもしくはそのネットワークドメインに関する制約(ドメイン制約)と、イベントの発生源となったプロセスおよびその先祖プロセスに関する制約(タイプ制約)とを論理積で組み合わせた制約条件を示しており、前記イベントがこの制約を満たす場合のみ、

(2) イベント制約の判定を行う。

#### 【0179】

DT制約について、より具体的に説明する。たとえば、以下のようにDT制約が記述されているものとする。

#### 【0180】

・タイプ制約:「プログラムT1」「プログラムT2」

・ドメイン制約:「133. 203. 1. 128」。

#### 【0181】

図40に示すように、これらの制約は以下の条件を指定する。

## 【0182】

・イベントの発生源である何らかのプロセスの先祖として、「プログラムT 2」のプロセスが存在すること。

## 【0183】

・「プログラムT 2」の親プロセスとして「プログラムT 1」のプロセスが存在すること。

## 【0184】

・「サーバプログラム」がIPアドレス「133. 203. 1. 128」のホストからアクセスを受けていること。

## 【0185】

なお、図40は「サーバプログラム」が「プログラムT 1」の先祖である場合を示しているが、一般的にはイベント発生源のプロセスおよびその先祖プロセスのいずれかが「サーバプログラム」であれば十分である。たとえば、「プロセスT 1」または「プロセスT 2」が「サーバプログラム」であってもよいし、イベント発生源のプロセスそのものが「サーバプログラム」であってもよい。

## 【0186】

(2) イベント制約と(3) 判定値は、第1実施形態におけるおとり装置2の正常動作定義と同じ意味である。すなわち、前記(2)はイベント名とパラメータ値についての正規表現の組である。攻撃検知部3702は、それらが前記イベントーコンテキスト対におけるイベントの名前およびパラメータ値と、合致するかどうかを判定する。

## 【0187】

また、前記(3)は、前記イベントが前記(2)に合致した場合に、攻撃検知部3702がそれを正常と判定するか、攻撃と判定するか、を定める値である。たとえば、正常と判定する場合の判定値を「ALLOW」、攻撃と判定する場合の判定値を「DENY」とする。なお、攻撃と判定する場合の判定値については、第1実施形態におけるおとり装置2と同様の攻撃種別を用いても良い。

## 【0188】

以下、特にDT制約について、より具体的な記述例と判定方法を示す。

## 【0189】

(ドメイン制約の記述例)

ドメイン制約は、例えば、IPアドレスの集合として記述できる。具体的には、1つのIPアドレスを10進3桁の数の4組「xxx. yyy. zzz. www」として記述し、「.」で区切ってIPアドレス集合の要素を列挙する。またその便法として、「xxx. yyy. zzz. www/vvv」(vvvはビットマスク)などの表記を許してもよい。あるいは、正規表現を用いることもできる。

## 【0190】

(タイプ制約の記述例)

また、タイプ制約は、例えば、実行形ファイル名に関する正規表現をもちいて記述できる。また、実行形ファイル名の連結によって、プロセスの親子関係を表現できるようにして、その正規表現を用いてもよい。

## 【0191】

具体的には、プロセスの親子関係を「<F(1)><F(2)>(中略)<F(N)>」(各F(i)は実行形ファイル名)という形式で表すことができる。このとき、それぞれの「<F(i)>」は、プロセスに関する制約であり、これにマッチする名前をもつ実行形ファイルの起動後のプロセスに相当する。また、その列挙は前方に記述されたプロセスを親とし、後方に書かれたプロセスをその直接の子とすることを示す。

## 【0192】

したがって、実行形ファイル「A」に相当するプロセスAの子として、実行形ファイル「B」に相当するプロセスBが、さらにその子として実行形ファイル「C」に相当するプロセスCが起動されている場合、プロセスA、B、Cの親子関係は「<A><B><C>」という文字列で表記される。

## 【0193】

こうしたプロセスの親子関係に関する正規表現をもって、タイプ制約とすることができる。具体的には、「<A>.\*<C>」というタイプ制約は、実行形ファイル「C」に相当するプロセスCが起動しており、その親プロセス(直接でなくともよい)が実行形ファイル「A」である場合に、マッチする。

## 【0194】

また特殊な例として、タイプ制約が「^」で始まる場合、その直後に記述されたプロセスが、プロセッサ201上のオペレーティングシステムの起動直後に生成されたプロセスである場合にマッチする。

## 【0195】

一般に、オペレーティングシステムは、唯一の初期プロセスをもち、起動直後のプロセスはすべて、その初期プロセスの直接の子となる。初期プロセスに相当する実行形ファイルが必ずしも存在するわけではないので、これを特殊記号「^」で表記することで、DT定義の汎用性を向上させることができる。

## 【0196】

別の特例として、タイプ制約が「\$」で終わる場合、「\$」の直前に指定されたプロセス「<F(N)>」が、イベント発生源であることを示す。

## 【0197】

(DT制約とイベントーコンテキスト対の比較)

DT制約の判定において、前記イベントーコンテキスト対との比較を行うが、その方法について、詳細に説明する。

## 50 【0198】

タイプ制約の判定は、コンテキストに含まれる逆方向リンクのうち、前記プロセスイベント管理キュー内のイベントを指すもの（以下、プロセスリンク）を選択する。前記リンク付けルールに従えば、任意のイベントにはその発生源であるプロセスの生成イベントを指すプロセスリンクが必ず存在する。

【0199】

そして、当該プロセスリンクを辿り、その先のイベントを参照して、実行形ファイル名をスタックに積む。こうしたステップを、プロセスリンクが存在しないイベント10に到達するまで繰り返す。

【0200】

一般的なオペレーティングシステムでは、任意のプロセスの先祖として初期プロセスが存在する。そのようなオペレーティングシステムがプロセッサ201上で動作している場合、初期プロセスは親プロセスをもたないため、かならず本ステップの繰り返しは終了する。

【0201】

もし、初期プロセスが存在しないようなオペレーティングシステムがプロセッサ201上で動作している場合、イベント管理部3701において、仮想的な初期プロセスの生成イベントを、プロセスイベント管理キューの先頭に配置するようにすればよい。

【0202】

前記ステップが終了した後、スタックに積まれた実行形ファイル名の系列は、前記初期プロセスから、前記イベント発生源のプロセスに至るまでのプロセス系列が得られる。当該プロセス系列は、プロセス間の親子関係を時系列順にならべたものに一致するので、当該プロセス系列と、タイプ制約とを比較することで、イベント系列20とタイプ制約が合致するか否かを判定できる。

【0203】

また、ドメイン制約の判定は、タイプ制約と同様にプロセスリンクをたどりながら、順次ネットワークイベント管理キューへの順方向リンクを参照していく。順方向リンクの先に、接続要求の受信イベントが見つければ、当該イベントに記載されているソースIPアドレスをアクセス元ホストのIPアドレスとみなし、探索を終了する。

【0204】

そして、前記IPアドレスと、ドメイン制約とを比較して合致するか否かを判定する。

【0205】

12.2.5.2) アラーム送信

以上のようにして、イベントーコンテキスト対とDT定義に記載された各ルールとの照合を繰り返し行い、

(1) DT制約および(2) イベント制約の全てに合致するかどうかを確認する(図34のステップF6)。もし、両方の制約に合致するルールが1つも無い場合は、デフォルト値として予めDT定義内に設定された判定値

を採用する。

【0206】

合致するルールがあれば、当該ルールの(3)判定値を参照して、前記イベントーコンテキスト対が攻撃であるかどうかを判定する(ステップF7)。

【0207】

そして、採用された判定値が許可(ALLOW)以外の場合、ただちにアラームを生成し、ファイアウォール装置1に送信する(ステップF8)。アラームの内容は第1実施形態におけるおとり装置2と同様に、少なくとも、前記アクセスのソースIPアドレスと、前記判定値を含み、その他、アクセス元のポート番号などを含めても良い。

【0208】

12.3) 効果

本実施形態におけるおとり装置37は、プロセッサ201が発生するイベントについて、イベント管理部3701でイベント間の因果関係の分析と履歴管理を行っている。これを用いて、攻撃検知部3702でアクセス元ホストや、サブシステムの呼び出し関係などを含めた、より詳細な正常動作定義が可能となる。これにより、複雑なサブシステム構成をもつサーバに対する攻撃検知性能を向上させると共に、保守作業の誤検知を低減させることができる。

【0209】

12.4) 具体例

本実施形態におけるおとり装置37の動作を具体例を用いて説明する。

【0210】

12.4.1) 構成

まず、おとり装置37のプロセッサ201上で、偽サービスとしてWWWサーバが動作しているものとする。そして、そのコンテンツ領域を、“C:\inetpub\wwwroot”ディレクトリ以下とする。また、WWWサーバのサブシステムとして、以下の2つのCGIモジュールを備えるものとする。

【0211】

(A) 登録CGI：顧客情報を顧客データベースに登録するCGI

(パス名：“C:\inetpub\scripts¥

regist.exe”)

(B) 出力CGI：顧客データベースの内容をHTMLに変換し、ブラウザ

から閲覧するCGI

(パス名：“C:\inetpub\scripts¥

view.exe”)

【0212】

ただし、出力CGIは専ら保守作業の1つとして利用されることを目的としており、内部ネットワーク4上の管理ドメイン”10.56.3.0/24”からのアクセ

スのみに応答することを要求されているものとする。また、別の保守作業として、FTPサーバを介したコンテンツの更新が想定されているものとする。

#### 【0213】

以下、クライアントとサーバとの間で行われる接続開始から要求データ送信完了までのIPパケット送受信をまとめて「アクセス」と呼ぶ。同様に、応答データ送信開始から接続終了までのIPパケット送受信をまとめて「(当該アクセスに対する) 応答」と呼ぶ。

#### 【0214】

こうした構成に対するDT定義の例として、図39に示すファイル4101のような設定がなされているものとする。ただし、「#」で始まる行はコメント行であり、無視されるものとする。

#### 【0215】

##### 12. 4. 2) 動作例1

具体的な動作の一例として、外部ネットワーク3上のクライアント(133. 201. 57. 2)から、内部ネットワーク4上のWWWサーバに対する不審アクセスがあって、それが正常である場合のおとり装置37の動作例を示す。

#### 【0216】

このとき、第1～第10実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置37に誘導され、偽サービス処理が開始される。

#### 【0217】

そして、おとり装置37のプロセッサ201上のWWWサーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。

#### 【0218】

(A) 133. 201. 57. 2からのアクセスを受信する。

#### 【0219】

(B) 子プロセスを生成する。

#### 【0220】

(C) 子プロセスで、当該アクセスにおける要求データに応じて、

例えば、

(C-1) コンテンツ領域に対するファイル入出力

(C-2) データベース操作のためのファイル入出力

を行う。

#### 【0221】

以下に、それぞれのステップごとにおとり装置37の内部動作を説明する。

#### 【0222】

##### 12. 4. 2. 1) 不審アクセスの受信

プロセッサ201上のWWWサーバが、不審アクセスを受信した直後、プロセッサ201からイベント管理部

3701に、イベント3501が伝達される(図41参照)。

#### 【0223】

イベント3501の内容には、少なくとも、イベント名(NW\_ACCEPT)、アクセス元IPアドレス(133. 201. 57. 2)、当該イベントの発生源であるプロセスであるWWWサーバのプロセスID(709)が記載される。その他、アクセス元のポート番号、TCP/UDPなどのプロトコル種別、要求データなどの情報を含めてもよい。

#### 【0224】

イベント3501を受け取ったイベント管理部3701は、直ちに図35に示すような対応表を参照して、イベント名「NW\_ACCEPT」のイベント種別を「ネットワーク」と判定し、前記イベントに追記する。そして、イベント種別「ネットワーク」に対応するイベント管理キューに、イベント3501を追加する。さらに、所定のリンク付けルールに従いイベント3501と関連する過去のイベントとの間にリンク付けを行う。

#### 【0225】

具体的には、図42を参照すると、イベント種別「プロセス」に対応するイベント管理キューから、前記イベント内に記載されたプロセスID(709)に相当するイベント名「PROC\_EXEC」または「PROC\_FORK」をもつイベント3601を検索する。このとき、最後尾から前方に向けてキュー走査を行い、最初にマッチするイベント3601を発見したとき、後の処理へ進む。

#### 【0226】

そして、イベント3601に対して、イベント3501への順方向リンク(図43の実線)を付加し、イベント3501に対して、イベント3601への逆方向リンク(図43の破線)を付加する。以下、リンクを図示する際は、逆方向リンクを省略する。

#### 【0227】

その後、イベント3501に関するイベントーコンテキスト対を、攻撃検知部3702に伝達する。

#### 【0228】

攻撃検知部3702では、まず、所定のDT定義ファイル4101を参照し、各ルールを抽出する。本例では、DT定義ファイル4101の先頭から前方に向かって1行ずつルールを抽出していく。なお、「#」で始まる行はコメントを意味し、コメントと空行はスキップされる。

#### 【0229】

まず、最初のルール(図39のルール1)が抽出される。本例の場合、ドメイン制約は「0.0.0.0/0」であり、これは任意のネットワークドメインにマッチする。また、タイプ制約は「<inetinfo.exe>」であり、WWWサ

サーバに相当するプロセスまたはその子プロセスにマッチする。

#### 【0230】

前記DT制約とイベント3501との照合のために、攻撃検知部3702は、まず、イベント3501のコンテキスト内の逆方向リンクをイベント管理部3701に入力して、リンク先のイベント3601の出力を受け

#### 【0231】

次に、イベント3601の内容を参照して、プロセスID「709」に相当するプログラム実行形ファイルのパス名「C:\Web\inetinfo.exe」を抽出する。さらに、イベント3601の逆方向リンクを先と同様にして、さらに親プロセスの生成イベントの取得を行おうとするが、本例では存在しない。したがって、イベント3601に相当するプロセスの親子関係を「<inetinfo.exe>」と判定し、前記タイプ制約「<inetinfo.exe>」にマッチすることを確認する。

#### 【0232】

次に、ドメイン制約との照合を行うため、再びイベント3501の内容を参照する。まず、イベント3501のイベント種別が「ネットワーク」であることを確認して、さらにイベント名が「NW\_ACCEPT」であることを確認する。

#### 【0233】

これにより、イベント3501自身がドメイン制約の対象となるので、さらにソースIPアドレスを参照して、「133.201.57.2」を取得する。この値は、前記ドメイン制約「0.0.0.0/0」にマッチする。

#### 【0234】

続けて、イベント制約の判定を行う。イベント名「FILE#WRITE」と、イベント3501のイベント名「NW\_ACCEPT」とを照合するが、この場合、一致しないので、当該ルールの照合処理を中断し、次のルール照合へ移る。

#### 【0235】

以下、同様にして、ルール抽出、DT制約の照合、イベント制約の照合を繰り返すが、本例の場合、いずれのルールにも合致しないため、デフォルトルール「DEFAULT;ALLOW」が採用され、イベント3501を「正常」と判定し、DT定義全体の照合を終了する。

#### 【0236】

##### 12.4.2.2) 子プロセスの生成

次に、プロセッサ201上のWWWサーバは前記不審アクセスの要求データを処理するために、子プロセスを生成する。一般に複数のアクセスを並行処理するサーバは、このように個々のアクセスに対する要求データ処理と応答処理を子プロセス側で行う。ただし、逐次的にアクセスを処理するサーバもあり、こうした場合には、直ちに要求データの処理に移る。また、子プロセスの代わりに子スレッドを作る場合もあるが、本例ではスレッド

と厳密な意味でのプロセスとを同等に、「(広義の)プロセス」として扱う。

#### 【0237】

プロセッサ201は、子プロセスの生成動作を受けて、イベント3801(図44参照)をイベント管理部3701に伝達する。イベント3801の内容には、少なくとも、イベント名「PROC#FORK」と、実行形ファイルのパス名「C:\Web\inetinfo.exe」と、生成された子プロセスのプロセスID(800)と、当該イベントの発生源であるプロセスID(709)が記載される。この他、スレッドと(狭義の)プロセスを区別するためのフラグなどを設けてもよい。

#### 【0238】

イベント3801の伝達を受けたイベント管理部3701は、前記イベント3501と同様にして、イベント3801のイベント種別(「プロセス」)を判定し、プロセスイベント管理キューへイベント3801を追加した後、イベント3601からイベント3801への順方向リンクと、イベント3801からイベント3601への逆方向リンクをつける(図44参照)。そして、イベント3801に関するイベントーコンテキスト対を攻撃検知部3202へ伝達する。

#### 【0239】

攻撃検知部3702では、先と同様に、イベント3801に関するイベントーコンテキスト対のリンクを探索して、イベント3801のDT判定を行う。その結果、イベント3801そのものがイベント種別「プロセス」であり、イベント3801の逆方向リンク先をイベント管理部3201から取得すると、イベント3601が得られる。したがって、イベント3801のタイプは「<inetinfo><inetinfo>」と判定される。

#### 【0240】

そして、再びイベント3801を参照するが、そのイベント種別は「ネットワーク」ではないので、イベント3801の順方向リンクを参照しようとする。しかし、イベント3801にはネットワークイベント管理キューへの順方向リンクがないので、イベント3801の逆方向リンク先をイベント管理部3701から取得する。イベント3801にはネットワークイベント管理キューへの順方向リンクがあるので、さらにその先にあるイベント3501を、イベント管理部3201から取得する。イベント3501は、イベント名が「NW\_ACCEPT」、ソースIPアドレスが「133.201.57.2」であるので、イベント3801のドメインを「133.201.57.2」と判定する。

#### 【0241】

なお、本例のように、プロセスの生成に係るイベントのドメイン決定時には、特別にその旨をイベント管理部3701に伝達して、イベント3801からイベント3501への逆方向リンクを付加するようにしてもよい。

このようにすることで、WWWサーバが子プロセスの実行中に、新たなアクセスを受信した場合でも、当該子プロセスが発生する後続イベントのドメインを誤ることはない。

#### 【0242】

次に、DT定義ファイル4401との照合を行うが、本例の場合、イベント3501と同様に、イベント3801は、いずれのルールにも完全に合致することなく、デフォルトの判定値（「DEFAULT;ALLOW」）が採用されるので、「正常」と判定される。

#### 【0243】

12.4.2.3) コンテンツ領域に対するファイル入出力

次に、プロセッサ201上のWWWサーバの子プロセスは前記不審アクセスの要求データを処理する。ここでは、まず、当該要求データが「GET /HTTP/1.0」である場合の動作例を示す。

#### 【0244】

前記要求データに対して、前記子プロセスは、コンテンツ領域内のファイル「C:\inetpub\wwwroot\default.htm」を読み込む。この動作を受けて、プロセッサ201はイベント3901（図45参照）をイベント管理部3701に伝達する。イベント3901の内容には、少なくとも、イベント名「FILE\_READ」、読み込むファイルのパス名「C:\inetpub\wwwroot\default.htm」、当該イベントの発生源である子プロセスのプロセスID（800）が記載される。この他、実際に読み込んだファイル内容などを含めても良い。

#### 【0245】

次に、イベント管理部3701は、イベント3901のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント3901を追加する。その後、イベント3801からイベント3901への順方向リンクと、イベント3901からイベント3801への逆方向リンクを付加する（図45参照）。その後、イベント3901に関するイベントーコンテキスト対を攻撃検知部3202に伝達する。

#### 【0246】

そして、攻撃検知部3702は、イベント3901に関するイベントーコンテキスト対に対するDT判定を行う。その結果、イベント3901のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「133.201.57.2」と判定する。

#### 【0247】

次に、攻撃検知部3702は、DT定義ファイル4101との照合を行う。本例の場合、以下のルール（図39のルール2）に合致し、その判定値が「ALLOW」であることから、「正常」と判定される。

#### 【0248】

0.0.0.0/0、<inetinfo.exe>、FILE#READ、C:\inet

info%.\*;

ALLOW

12.4.2.4) データベース操作

別の要求データの例として、「GET /cgi-bin/regist.exe name=someoneHTTP/1.0」である場合の動作例を示す。

#### 【0249】

(ア) CGIの起動

この要求データに対して、前記子プロセスは、まず、前記登録CGIを起動して、新たな孫プロセスを生成する。また、URLパラメータ「name=someone」は環境変数「QUERY#STRING」に格納されているものとする。

#### 【0250】

この動作を受けて、プロセッサ201はイベント4001（図46参照）をイベント管理部3701に伝達する。イベント4001の内容には、少なくとも、イベント名「PROC#EXEC」と、実行形ファイルのパス名「C:\inetpub\scripts\regist.exe」と、前記孫プロセスのプロセスID（801）と、当該イベントの発生源である前記子プロセスのプロセスID（800）とが記載される。この他、環境変数の情報などを含めてもよい。

#### 【0251】

次に、図46を参照すると、イベント管理部3701は、イベント4001のイベント種別を「プロセス」と判定し、プロセスイベント管理キューにイベント4001を追加する。その後、イベント3801からイベント4001への順方向リンクと、イベント4001からイベント3801への逆方向リンクを付加し、イベント4001に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

#### 【0252】

そして、攻撃検知部3702は、イベント4001に関するイベントーコンテキスト対に対して、イベント3901と同様にDT判定を行う。その結果、イベント4001のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「133.201.57.2」と判定する。

#### 【0253】

次に、攻撃検知部3702は、DT定義との照合を行う。本例の場合、合致するルールがないので、デフォルトルールの判定値「ALLOW」を採用して、正常と判定する。

#### 【0254】

(イ) CGIの動作

続けて、前記登録CGIがデータベース出力を行う。本例では、登録CGIが操作するデータベースを「C:\data\client.db」ファイルとする。

#### 【0255】

データベース出力の具体例として、登録CGIは前記環境変数「QUERY#STRING」の値を読み取り、その値「na

me=someone」に改行記号を加えた文字列を前記データベースの末尾に追記するものとする。

【0256】

この動作を受けて、プロセッサ201はイベント4101（図47参照）をイベント管理部3701に伝達する。イベント4101の内容には、少なくとも、イベント名「FILE#WRITE」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記孫プロセスのプロセスID（801）とが記載される。その他、書き出したデータの内容などを含めてもよい。

【0257】

次に、図47を参照すると、イベント管理部3701は、イベント4101のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント4101を追加する。その後、イベント4001からイベント4101への順方向リンクと、イベント4101からイベント4001への逆方向リンクを付加し、イベント4101に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

【0258】

そして、攻撃検知部3702は、イベント4101に関するイベントーコンテキスト対に対して、DT判定を行う。その結果、イベント4101のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「133.201.57.2」と判定する。

【0259】

次に、攻撃検知部3702は、DT定義ファイル4101との照合を行う。本例の場合、以下のルール（図39のルール3）に合致するので、その判定値「ALLOW」を採用して、正常と判定する。

【0260】

0.0.0/0、<inetinfo.exe><regist.exe>\$、FILE#WRITE、

C:\data\client.db; ALLOW

12.4.3) 動作例2

具体的な動作の別の例として、外部ネットワーク3上のクライアント（133.201.57.2）から、内部ネットワーク4上のWWWサーバに対する不審アクセスがあって、それが攻撃である場合を示す。

【0261】

このとき、第1～第10実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置37に誘導され、偽サービス処理が行われる。

【0262】

その後、おとり装置37のプロセッサ201上のWWWサーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。

【0263】

(A) 133.201.57.2からのアクセスを受信する。

【0264】

(B) 子プロセスを生成する。

【0265】

(C) 子プロセスで、当該アクセスにおける不正な要求データに応じて、所定の処理を行う。例えば、

(C-1) コンテンツ領域に対する不正ファイル書き出し

(C-2) データベースに対する不正アクセスなどを行う。

10 【0266】

上記(A)、(B)は前記動作例1と同様であるため、ここでは攻撃時の動作(C-1)、(C-2)のみについて具体例を示す。

【0267】

12.4.3.1) コンテンツ領域に対する不正ファイル書き出し

WWWサーバまたはそのサブシステム（登録CGI・出力CGI）などに脆弱性が存在するものとする。今、登録CGIに脆弱性が存在し、「GET/cgi-bin/regist.exe path=C:\inetpub\wwwroot\default.htm&data=abcd」というアクセスがあった場合に、コンテンツ領域内のファイル「C:\inetpub\wwwroot\default.htm」に対して、データ「abcd」が書き込まれるものとする。

20

【0268】

前記不正アクセスがあった場合、前記動作(C-1)が行われ、プロセッサ201はイベント4901（図48参照）をイベント管理部3701に伝達する。イベント4901の内容には、少なくとも、イベント名「FILE#WRITE」と、実行形ファイルのパス名「C:\inetpub\wwwroot\default.htm」と、当該イベント発生源である前記孫プロセスのプロセスID（801）とが記載される。

30

【0269】

次に、イベント管理部3701は、イベント4901のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント4901を追加する（図48参照）。その後、イベント4001からイベント4901への順方向リンクと、イベント4901からイベント4001への逆方向リンクを付加し、イベント4901に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

40

【0270】

そして、攻撃検知部3702は、イベント4901に関するイベントーコンテキスト対に対してDT判定を行う。その結果、イベント4901のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「133.201.57.2」と判定する。

【0271】

次に、攻撃検知部3702は、DT定義との照合を行う。本例の場合、以下のルール（図39のルール6）に合致するので、その判定値「DENY」を採用し、攻撃

50

があったものと判定する。

【0272】

0.0.0.0/0、<inetinfo.exe>、FILE#WRITE、.\*; DENY

そして、攻撃検知部3702は、攻撃元ホスト「133.201.57.2」を含むアラームを直ちに生成して、前記ファイアウォール装置1へ送信する。

【0273】

なお、WWWサーバもしくはそのサブシステムの脆弱性を介した不正なファイル書き込みがあった場合、すべて前記と同様にして攻撃であると判定される。

【0274】

また、WWWサーバ以外のサーバ、例えばFTPサーバを介したコンテンツ領域への書き込みがあった場合、以下のルール（図39のルール5）に合致しない限り、すなわち、管理ドメインからの正当な保守作業でない限り、

10.56.192.0/24、.<ftpd.exe>+\$.、FILE#WRITE、C:\inetpub\wwwroot\.\*; ALLOW

以下のルール（図39のルール8）により、攻撃であると判定される。

【0275】

0.0.0.0/0、.\*、FILE#WRITE、C:\inetpub\wwwroot\.\*; DENY

12.4.3.2) データベースへの不正アクセス  
WWWサーバまたはそのサブシステム（登録CGI・出力CGI）などに脆弱性が存在するものとし、「GET/cgi-bin/.%c1%c9../data/client.db HTTP/1.0」というアクセスによって、前記顧客データベースを窃取されるものとする。

【0276】

前記不正アクセスがあった場合、前記動作が行われたのを受けて、プロセッサ201はイベント5001（図49参照）をイベント管理部3701に伝達する。イベント5001の内容には、少なくとも、イベント名「FILE#READ」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記子プロセスのプロセスID（800）とが記載される。

【0277】

次に、イベント管理部3701は、イベント5001のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント5001を追加する。その後、イベント3801からイベント5001への順方向リンクと、イベント5001からイベント3801への逆方向リンクを付加し、イベント5001に関するイベントーコンテキスト対を攻撃検知部3702に伝達する。

【0278】

そして、攻撃検知部3702は、イベント5001のイベントーコンテキスト対に対してDT判定を行う。そ

の結果、イベント5001のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「133.201.57.2」と判定する。

【0279】

次に、攻撃検知部3702は、DT定義との照合を行う。本例の場合、以下のルール（図39のルール7）に合致するので、その判定値「DENY」を採用し、攻撃があったものと判定する。

【0280】

0.0.0.0/0、.\*、FILE#READ|FILE#WRITE、C:\data\.\*; DENY

そして、攻撃検知部3702は、攻撃元ホスト「133.201.57.2」を含むアラームを直ちに生成して、前記ファイアウォール装置1へ送信する。

【0281】

（第13実施形態）

13.1) 構成

図50は、本発明の第13実施形態におけるファイアウォール装置のブロック図である。本実施形態におけるファイアウォール装置51は、第2実施形態におけるファイアウォール装置5の誘導部503および信頼度管理部502に代えて、仮想サーバ部5101および信頼度管理部5102を備える。

【0282】

図51を参照すると、仮想サーバ部5101は、接続管理部5201と、第1入力バッファ5202および第1出力バッファ5203と、第2入力バッファ5204および第2出力バッファ5205とを有する。

【0283】

30 接続管理部5201は、パケットフィルタ101から伝達された各アクセスに含まれる要求データを信頼度管理部5102に輸入し、その信頼度を取得する。また、その信頼度に応じて、第1入力バッファ5202または第2入力バッファ5204への要求データ転送処理や、第1出力バッファ5203または第2出力バッファ5205からの応答データ読み取り処理などを行う。

【0284】

第1入力バッファ5202および第1出力バッファ5203は、第1の内部通信インターフェース104を内部ネットワーク4に接続されており、それぞれサーバ装置への要求データと、サーバ装置からの応答データを一時格納する。

【0285】

第2入力バッファ5204および第2出力バッファ5205は、おとり装置2に接続されており、それぞれおとり装置2への要求データと、おとり装置2からの応答データを一時格納する。また、信頼度管理部5102は、仮想サーバ部5101の接続管理部5201からの要求データ入力に応じて、その信頼度を出力する。

【0286】



## 13. 2) 動作

図52は、第13実施形態におけるファイアウォール装置33のフローチャートである。

## 【0287】

## 13. 2. 1) 仮接続

図52において、まず、ファイアウォール装置33がインターネット3上のあるホストから新たな接続を要求する入力IPパケットを受信して、第2実施形態におけるファイアウォール装置5と同様に、パケットフィルタ101とアクセス制御リスト管理部102とによって、その通過を認められた場合には、仮想サーバ5101の接続管理部5101は、前記ホストとの間に仮の接続を確立する(ステップG1)。

## 【0288】

## 13. 2. 2) 要求データの一時格納

その後、前記インターネット3上のホストから内部ネットワーク4上のサーバに対する要求データを受信する(ステップG2)。そして、接続管理部5201は、当該要求データを第1入力バッファ5202と第2入力バッファ5204とに伝達して、一時格納する(ステップG3)。

## 【0289】

## 13. 2. 3) 信頼度判定

そして、前記要求データを信頼度管理部5102に入力し、その信頼度 $c$ を取得し(ステップG4)、所定の閾値 $T$ と比較を行う(ステップG5)。

## 【0290】

信頼度管理部5102における信頼度の計算方法としては、例えば、要求データをバイトデータの系列パターンとみなして、統計的なパターン解析によって、「頻繁に見られる要求データ」との類似度を計算し、当該類似度をもって信頼度 $c$ とする方法がある。

## 【0291】

また、単に図53に示すような、過去に入力された要求データと信頼度との組を管理するためのテーブルを保持し、新たな要求データの入力があるたびに、当該テーブルを参照して、信頼度を求める方法を用いてもよい。より具体的には、ステップG8-2でおとり装置2によって正常であることが確認された場合にのみ信頼度を1とし、それ以外の場合、特にステップG8-3において、攻撃であることが確認された場合には、信頼度を0とし、以降この信頼度を再利用する方法を用いてもよい。

## 【0292】

さらに、前記テーブルに要求データを直接格納するのではなく、要求データの一方方向性ハッシュ関数値を格納する方法を用いてもよい。この場合、既知の要求データが再度入力された場合、その一方方向性ハッシュ関数値としても一致するため、その信頼度を正しく取得できる。さらに、要求データのサイズが非常に大きなものになり

得る場合でも、一方方向性ハッシュ関数値は常に一定のサイズであるため、メモリ効率が良い。ただし、異なる要求データに対する一方方向性ハッシュ関数値が一致する(=衝突する)場合があるが、一般に一方方向性ハッシュ関数値が一致する異なる2つの要求データ(特に、一方が正常でもう一方が攻撃であるような場合)を見つけることは困難とされるので、実用上の危険性は極めて小さい。

## 【0293】

## 13. 2. 3. 1) 要求データを信頼した場合

もし、 $c \geq T$ であれば(ステップG5のY)、前記要求データを信頼できるものと判定し、第1入力バッファ5202と、第2入力バッファ5204とに、要求データの転送を指示する(ステップG6-1)。この指示を受けた第1入力バッファ5202は、直ちに格納済み要求データを、第1の内部通信インターフェース104を介して、内部ネットワーク4上のサーバに転送する。同様に、第2入力バッファ5104は、格納済み要求データを、第2の内部通信インターフェース105を介して、おとり装置2に転送する。

## 【0294】

## 13. 2. 3. 2) 応答データの確認

その後、第1の内部通信インターフェース104を介して、内部ネットワーク4上のサーバから応答データを受信したとき、第1出力バッファ5203は当該応答データを一時格納し、接続管理部5201に応答のあった旨を伝える(ステップG7-1)。

## 【0295】

## 13. 2. 3. 3) 応答データの転送

接続管理部5201は、第1出力バッファ5203からデータ受信を伝達された後、直ちに前記ホストに向けて、第1出力バッファ5203に格納された応答データを転送する(ステップG8-1)。

## 【0296】

## 13. 2. 4) 要求データを不審とした場合

一方、ステップG5の後、 $c < T$ であれば(ステップG5のN)、前記要求データを不審であると判定し、第2入力バッファ5204のみに、要求データの転送を指示する(ステップG6-2)。第2入力バッファ5204は、この指示を受けて、直ちに第2の内部通信インターフェース105を介して、おとり装置2へ前記要求データを転送する。

## 【0297】

## 13. 2. 4. 1) 攻撃検知

そして、おとり装置2は第2実施形態と同様にして、攻撃の有無を判定する(ステップG7-2)。

## 【0298】

## 13. 2. 4. 2) 攻撃が検知された場合

攻撃があった場合には(ステップG7-2のY)、その旨を伝えるアラームを生成して、ファイアウォール装

置51へ送信する。制御インタフェース106を介して、当該アラームを受信したファイアウォール装置33は、第2実施形態におけるファイアウォール装置5と同様に、防御ルール判定部107から、信頼度管理部5102に前記ホストから攻撃のあったことを伝達すると共に、アクセス制御リスト管理部102にアクセス制御ルールの更新を指示して、前記接続を遮断する(ステップG8-3)。

#### 【0299】

13. 2. 4. 3) 攻撃が検知されなかった場合  
一方、所定のタイムアウト時間内に攻撃が検知されなかった場合には(ステップG7-2のN)、信頼度管理部5102は接続管理部5201へアラームを伝達する。接続管理部5201は、当該アラームを受けて、第1入力バッファ5202へ格納済み要求データの転送を指示する(ステップG8-2)。

#### 【0300】

なお、前記タイムアウト時間は、500ミリ秒程度の時間を設定すれば通常十分であるが、入力IPパケットがファイアウォール装置51に到達する時間間隔の平均値などをもって、適応的に変化させるようにしてもよい。

#### 【0301】

その後、第1の内部通信インタフェース104を介して、内部ネットワーク4上のサーバから応答データを受信したとき、第1出力バッファ5203は当該応答データを一時格納し、接続管理部5201に応答のあった旨を伝える(ステップG7-1)。

#### 【0302】

接続管理部5201は、第1出力バッファ5203からデータ受信を伝達された後、直ちに前記ホストに向けて、第1出力バッファ5203に格納された応答データを転送する(ステップG8-1)。

#### 【0303】

##### 13. 3) 効果

第13実施形態におけるファイアウォール装置51によれば、1回の接続について、複数の要求データ $r(1)$ 、 $r(2)$ 、...、 $r(n)$ があつて、その途中のある要求データ $r(i)$ が不審とされるような場合、おとり装置2で当該要求データ $r(i)$ に対するサーバ動作から攻撃が検知されなかったとき、 $r(i)$ は内部ネットワーク4上の正規サーバへ必ず転送されるので、 $r(1) \sim r(n)$ の全要求データが正しい順序で正規サーバに到達することを保証できる。

#### 【0304】

一方、おとり装置2で攻撃が検知されたとき、直ちに前記接続が遮断されるので、前記要求データ $r(i)$ を含め、それ以降の要求データは一切、前記正規サーバに到達しないことを保証できる。

#### 【0305】

こうした性質は、データベースと連携するWWWサーバ(いわゆる「3層システム」)や、Telnetサーバや、FTPサーバなどと、それぞれのクライアントとの間で行われるように、1回の接続につき、複数の要求と応答が繰り返されるようなプロトコル(=ステートフルプロトコル)に従うサービスの保護に適する。

#### 【0306】

こうしたサービスにおいては、要求データ系列の順序が異なると、正しいサービス提供が保証できない。また、前記のように、攻撃用データを要求データ系列の一部として含むような場合にも、それまでの要求データ系列の順序が異なると、当該攻撃用データによるサーバの異常動作が予測できない場合がある。

#### 【0307】

したがって、本実施形態におけるファイアウォール装置50とおとり装置2との組み合わせによる攻撃防御システムは、ステートフルプロトコルに従うサービスについて、その正常動作および異常動作を誤りなく判定し、攻撃を確実に防御することができる。

#### 【0308】

また、WWWサーバによる静的コンテンツ提供のような、ステートレスプロトコルを対象とする場合でも、本実施例による誘導方法によれば、インターネット3上のホストに転送される応答データは常に正規サーバの出力する応答データである。したがって、静的コンテンツの改ざんなどがおとり装置2で発生していた場合でも、改ざんされたコンテンツが前記ホストに到達することが一切なく、常に正しいコンテンツの提供が保証できる。

#### 【0309】

##### 13. 4) 具体例

##### 13. 4. 1) 構成

図54を参照すると、本実施例は、インターネット3上のFTPクライアント302と、内部ネットワーク4上のFTPサーバ402と、ファイアウォール装置51と、おとり装置2とから構成される。

#### 【0310】

FTPクライアント302は、FTPサーバ402に向けていくつかの要求データを送信するが、それらは全て、ファイアウォール装置51で中継される。また、ファイアウォール装置51は、FTPクライアント302から入力される要求データをおとり装置2へも転送する。さらに、おとり装置2のプロセッサ201上では、FTPサーバ402と同じFTPサービスが提供されている。

#### 【0311】

##### 13. 4. 2) 動作

FTPクライアント302は、FTPサーバ402に向けて、要求データを順次送信するが、本実施例では、FTPクライアント302が、

##### 50 1) 匿名ログイン

2) ファイルアップロード  
 を行う場合の、ファイアウォール装置51の動作例を示す。

#### 【0312】

また、FTPサーバ402とおとり装置2とは、非常に長いファイル名を処理したときにバッファオーバーフローを起こして、シェルが不正に操作される、という共通の脆弱性をもつものとする。

#### 【0313】

さらに、おとり装置2の攻撃検知部202には、プロセッサ201で動作するFTPサーバがシェルを起動することを禁止するような正常動作定義がなされているものとする。

#### 【0314】

##### 13.4.2.1) 仮接続

まず、FTPクライアント302は、FTPサーバ402へのログインに先立って、所定のTCP接続を確立するため、FTPサーバ402に向けてSYNパケットを送信する。

#### 【0315】

当該SYNパケットが、ファイアウォール装置51に到達したとき、ファイアウォール装置51の仮想サーバ5101は、FTPサーバ402に代わって、前記SYNパケットに対応するSYN-ACKパケットを応答する。

#### 【0316】

その後、FTPクライアント302は、さらにACKパケットをFTPサーバ402へ向けて送信する。当該ACKパケットがファイアウォール装置51に到達したとき、仮想サーバ5101は、新たなTCP接続が確立したものと判定する。

#### 【0317】

そして、仮想サーバ5101の接続管理部5201は、FTPサーバ402と、おとり装置2とに対して、FTPクライアント302に代わって、個別にTCP接続を確立する。

#### 【0318】

##### 13.4.2.2) 匿名ログイン

次に、FTPクライアント302は、FTPサーバ402へ向けて、匿名ログインを行うための要求データを送信する。

#### 【0319】

一般に、FTPサーバに対する匿名ログインは、以下のような2個の要求データを送信する。

#### 【0320】

・第1の要求データ(r1)：ユーザ名を示すものであり、一般に「anonymous」である。

#### 【0321】

・第2の要求データ(r2)：パスワードを示すものであり、一般に「user@domain」の形式をもつメールアドレス

スである。

#### 【0322】

第1の要求データr1が、ファイアウォール装置51に到達したとき、仮想サーバ5101の接続管理部5201は、まず、第1の要求データr1を第1入力バッファ5202と、第2入力バッファ5204とに伝達し、一時格納する。

#### 【0323】

その後、第1の要求データr1を信頼度管理部5102に入力し、その信頼度を取得する。このとき、信頼度管理部5102は、例えば、図53のような信頼度管理テーブルに対して、第1の要求データr1をキーとして信頼度を検索する。このとき、第1の要求データr1のエントリがあれば、その信頼度c1を、接続管理部5201に出力する。もし、第1の要求データr1のエントリが無ければ、信頼度の初期値「0」をもつ、新たなエントリを追加し(図55の網掛け部)、信頼度0を接続管理部5201に出力する。本実施例では、すでに第1の要求データr1のエントリが存在し、その信頼度が「1」であるものとする。

#### 【0324】

そして、接続管理部5201は、所定の閾値と前記信頼度を比較する。本実施例では、閾値を1とする。したがって、接続管理部5201は、第1の要求データr1を信頼し、第1入力バッファ5202と、第2入力バッファ5204とに、第1の要求データr1の転送を指示する。

#### 【0325】

転送を指示された第1入力バッファ5202および第2入力バッファ5204は、それぞれ、FTPサーバ402およびおとり装置2へ、第1の要求データr1を転送する。

#### 【0326】

その後、第1の要求データr1を受信したFTPサーバ402は、パスワードの入力を求める応答データs1をFTPクライアント302へ向けて送信する。応答データs1がファイアウォール装置51に到達したとき、応答データs1は一旦第1出力バッファ5203に格納される。そして、第1出力バッファ5203は、新たな応答データを受信した旨を、接続管理部5201に伝達する。

#### 【0327】

そして、接続管理部5201は、第1出力バッファ5203に格納された応答データs1を、FTPクライアント302に向けて転送する。なお、おとり装置2からも応答データs1が送信され、第2出力バッファ5205がs1を格納し、接続管理部5201に応答データ受信を伝達するが、本実施例における接続管理部5201は、これを無視する。

#### 【0328】

以上のようにして、FTPクライアント302からF

FTPサーバ402へ向けて送信された要求データr1は、適切にFTPサーバ402およびおとり装置2へ転送される。

#### 【0329】

次に、パスワード入力である要求データr2についても、信頼度管理部5102は、その信頼度を「1」と出力するものとする。したがって、r2はr1と同様にして、FTPサーバ402およびおとり装置2へ転送される。こうして、FTPクライアント302は、FTPサーバ402およびおとり装置2の双方に対して、匿名ログインを完了することができる。

#### 【0330】

13. 4. 2. 3) ファイルアップロード  
匿名ログインを完了したFTPクライアント302は、ファイルアップロードを行う。FTPサービスにおけるファイルアップロードは、以下の形式のコマンドを要求データに含めることで行われる。

#### 【0331】

「PUT <ファイル名>」。

#### 【0332】

ここで、以下の2種類の要求データを考える。

#### 【0333】

(A) r3-1: 「PUT FILE. TXT」

(B) r3-2: 「PUT XXXXXXXX・・・<シェルコード>」。

#### 【0334】

r3-1は、「FILE. TXT」という名前のファイルをFTPサーバ402にアップロードしようとするものであり、正常な要求データであるとする。一方r3-2は、FTPサーバ402にバッファオーバーフローを引き起こさせて、ファイル名の一部として含められたシェルコードを不正にFTPサーバ402内のシェルに実行させようとするものであるとする。

#### 【0335】

13. 4. 2. 3. 1) 正常な要求データr3-1が入力された場合

まず、FTPクライアント302から要求データr3-1が送信された場合を示す。

#### 【0336】

要求データr3-1がファイアウォール装置51に到達した際、前記要求データr1と同様にして、接続管理部5201によって、第1入力バッファ5202および第2入力バッファ5204とに格納され、要求データr3-1が信頼度管理部5102に入力される。

#### 【0337】

信頼度管理部5102は、前記信頼度管理テーブルを参照するが、このとき、要求データr3-1のエントリがないものとする。この場合、信頼度管理部5102は、信頼度管理テーブルに、要求データr3-1のエントリを新たに追加する。また、要求データr3-1の信

頼度として、所定の初期値「0」を設定し、「0」を接続管理部5201に出力する。

#### 【0338】

接続管理部5201は、要求データr3-1の信頼度「0」を取得したのち、閾値「1」との比較を行って、閾値より小さな信頼度であることを確認し、要求データr3-1を不審とみなす。そして、第2入力バッファ5204のみに、要求データr3-1の転送を指示する。

#### 【0339】

第2入力バッファ5204は、前記転送指示を受けて、おとり装置2に要求データr3-1を転送する。

#### 【0340】

おとり装置2は、要求データr3-1を受信して、ファイル「FILE. TXT」を保存した後、保存が完了した旨を伝える応答データs3-1を送信する。

#### 【0341】

その後、応答データs3-1は、ファイアウォール装置51に到達し、第2出力バッファ5205に格納され、第2出力バッファ5205は、その旨を接続管理部5201に通知する。そして、接続管理部5201は、信頼度管理部5102に要求データr3-1が正常であることを通知し、信頼度管理部5102は、前記信頼度管理テーブルを更新して、要求データr3-1の信頼度を「1」にする。

#### 【0342】

さらに、接続管理部5201は、第1入力バッファ5202に要求データr3-1の転送を指示して、第1入力バッファ5202に要求データr3-1をFTPサーバ402に転送させる。

#### 【0343】

その後、FTPサーバ402は、ファイル「FILE. TXT」を保存し、その完了を伝える応答データs3-1を送信する。

#### 【0344】

FTPサーバ402からの応答データs3-1は、第1出力バッファ5203に格納され、第1出力バッファ5203は、その旨を接続管理部5201に通知する。そして、接続管理部5201は、s3-1をFTPクライアント302に転送する(図56参照)。

#### 【0345】

以上のようにして、FTPクライアント302から送信されたファイル「FILE. TXT」は、FTPサーバ402およびおとり装置2に適切に保存される。

#### 【0346】

13. 4. 2. 3. 2) 要求データr3-2が入力された場合

次に、FTPクライアント302から不正な要求データr3-2が送信された場合を示す。

#### 【0347】

要求データr3-2がファイアウォール装置51に到

達した際、前記要求データr3-1と同様にして、接続管理部5201によって、第1入力バッファ5202および第2入力バッファ5204とに格納され、要求データr3-2が信頼度管理部5102に入力される。

#### 【0348】

信頼度管理部5102は、前記信頼度管理テーブルを参照するが、このとき、やはり、要求データr3-2のエントリがないものとする。この場合、信頼度管理部5002は、信頼度管理テーブルに、要求データr3-1のエントリを新たに追加する。また、要求データr3-2の信頼度として、所定の初期値「0」を設定し、「0」を接続管理部5201に出力する。

#### 【0349】

接続管理部5201は、要求データr3-2の信頼度「0」を取得したのち、閾値「1」との比較を行って、閾値より小さな信頼度であることを確認し、要求データr3-2を不審とみなす。

#### 【0350】

そして、第2入力バッファ5204のみに、要求データr3-2の転送を指示する。第2入力バッファ5204は、前記転送指示を受けて、おとり装置2に要求データr3-2を転送する。

#### 【0351】

おとり装置2が要求データr3-2を受信すると、プロセッサ201上で、(偽の)FTPサーバはバッファオーバーフローによってシェルを起動し、要求データr3-2に含まれる不正なシェルコードを実行しようとする。おとり装置2の攻撃検知部202は、当該シェル起動を攻撃と検知し、直ちにアラームをファイアウォール装置51に送信する。

#### 【0352】

前記アラームを受信したファイアウォール装置51は、まず、防御ルール判定部107と、アクセス制御リスト管理部102と、パケットフィルタ101とによって、第1実施形態におけるファイアウォール装置1と同様に、FTPクライアント302からの以降のアクセスを遮断する。また、防御ルール判定部107は、アラームの受信を接続管理部5201にも通知する。

#### 【0353】

アラーム受信通知を受けた接続管理部5201は、ただちにFTPクライアント302との接続を遮断する。また、望ましくは、第1入力バッファ5202に格納されたr3-2を消去する。

#### 【0354】

以上のようにして、不正な要求データr3-2は、到達するとしてもおとり装置2に限られ、FTPサーバ402に到達しない(図57参照)。

#### 【0355】

##### (第14実施形態)

図58に示すように、内部ネットワーク4上のサーバ

(例えばFTPサーバ402)からおとり装置2へ少なくともファイルシステムの内容を複写するミラーリング装置5901をさらに備えてもよい。

#### 【0356】

おとり装置2で攻撃が検知されファイアウォール装置51の防御ルール判定部107にアラームが伝達された際、防御ルール判定部107は、さらにミラーリング装置5901にもアラーム受信を通知する。

#### 【0357】

当該通知を受けたミラーリング装置5901は、前記内部ネットワーク4上のサーバのファイルシステム4021を読み取り、その内容をおとり装置2上のファイルシステム2011へ複写する。こうすることにより、おとり装置2上で不正なファイル書き込みが発生しても、その被害をリアルタイムに復旧することができる。

#### 【0358】

本実施形態ではファイルシステムを具体例として挙げたが、その他に、さらにメモリモジュールの内容を複写するようにしてメモリ内の異常を復旧するようにしてもよい。また、おとり装置2から送信されるアラームに、書換えられたファイルのパス名、あるいは、メモリ領域を記載するようにして、被害を受けた部分のみを複写できるようにしてもよい。

#### 【0359】

##### (第15実施形態)

図59は、本発明の第15実施形態におけるファイアウォール装置の概略的構成図である。本実施形態におけるファイアウォール装置62は、第13実施形態におけるファイアウォール装置51の仮想サーバ5101の前段に暗号処理部6201を備える。

#### 【0360】

暗号処理部6201は、パケットフィルタ101から得られた暗号化入力IPパケットを復号し、復号された入力IPパケットを仮想サーバ5101に伝達する。また、仮想サーバ5101から得られた出力IPパケットを暗号化し、暗号化出力IPパケットをパケットフィルタ101に伝達する。

#### 【0361】

このようにすることで、インターネット3および内部ネットワーク4との間で暗号化通信が行われる場合にも、おとり装置への誘導を行うことができる。

#### 【0362】

##### (第16実施形態)

上記第1～第15実施形態では、誘導部(または仮想サーバ部)、防御ルール判定部、パケットフィルタ、および、アクセス制御リスト管理部が一つのユニットになったファイアウォール装置を例示したが、本発明はこれに限定されるものではない。

#### 【0363】

たとえば、次のようにハードウェア的に2ユニットで

構成し、それらをネットワークで接続することもできる。

#### 【0364】

・少なくともパケットフィルタおよびアクセス制御リスト管理部を有するファイアウォール装置

・少なくとも誘導部（または仮想サーバ部）および防御ルール判定部を有するスイッチ装置。

#### 【0365】

従来のファイアウォール装置は、遠隔からアクセス制御リストの部分的更新を行う機能を有していることが多いので、既に設置済みのファイアウォール装置に加えて、上記スイッチ装置を設置することで、第1～第14実施形態における1ユニットのファイアウォール装置と同等の機能を実現できるというメリットがある。

#### 【0366】

図60は本発明の第16実施形態による攻撃防御システムの概略的構成図である。本実施形態において、ファイアウォール装置7001にはパケットフィルタ101およびアクセス制御リスト管理部102が設けられ、スイッチ装置7002には誘導部501、信頼度管理部502および防御ルール判定部107が設けられている。パケットフィルタ101と誘導部501との間、および、アクセス制御リスト管理部102と防御ルール判定部107との間をネットワークを介して接続することで、第1～第15実施形態による攻撃防御システムを実現することができる。

#### 【0367】

（第17実施形態）

##### 17. 1) 構成

図61は、本発明の第17実施形態による攻撃防御システムの概略的構成図である。本実施形態における攻撃防御システムは、ファイアウォール装置80と、サーバ装置401と、複数のおとり装置2(1)～2(k)から構成されるおとりクラスタ21と、から構成される。

#### 【0368】

ファイアウォール装置80は、少なくとも誘導部8001、サーバ管理部8002、および、信頼度管理部502を有する。誘導部8001は、すでに述べた手順により、新規に受信したアクセスに関する信頼度を信頼度管理部502からを受け取り、さらに、当該信頼度をサーバ管理部8002へ渡して適切なおとり装置2(i)の識別子を受け取る。誘導部8001は、受け取った識別子で指示されたおとり装置2(i)もしくは内部ネットワークへ受信したアクセスを転送する。

#### 【0369】

サーバ管理部8002は、おとりクラスタ21に含まれるおとり装置2(1)～2(k)の識別子と必須信頼度との対応関係を示す参照表8003を内部的に備えており、誘導部8001からの信頼度の入力を受けて、参照表から適切な識別子を選択し、選択された識別子を誘

導部8001へ返す。

#### 【0370】

図62は、サーバ管理部8002が有する参照表8003の一例を示す模式図である。ここでは、おとり装置2(1)～2(k)にそれぞれ対応するサーバ識別子D1～Dkと必須信頼度M1～Mkとの対応が格納されている。

#### 【0371】

##### 17. 2) 動作

図63は、本発明の第17実施形態による攻撃防御システムの動作を示すフローチャートである。ファイアウォール装置80がサーバ装置401へ向かうパケットpを受信すると、誘導部8001は、まず入力パケットpの少なくともヘッダを信頼度管理部502へ出力し、パケットpに対する信頼度 $\tau[p]$ を受け取る（ステップ11）。

#### 【0372】

続いて、誘導部8001は、信頼度 $\tau[p]$ をサーバ管理部8002へ出力し、少なくとも1つの識別子を受け取る。このとき、サーバ管理部8002は、参照表8003の必須信頼度の列を走査し、受け取った信頼度 $\tau[p]$ 以下の必須信頼度に対応する識別子を検索する（ステップ12および13）。

#### 【0373】

対応する識別子を発見できなかった場合は（ステップ13のN）、少なくともサーバ装置401に割り当てられた所定の識別子および必須信頼度Nの組を仮の検索結果としてする（ステップ14）。この場合、さらに、おとりクラスタ21上の全てのおとり装置の識別子D1～Dkの系列を検索結果に加えてもよい。なお、サーバ装置401の必須信頼度Nは、参照表8003の必須信頼度M1～Mkの最大値を越える値であるものとする（ $N > \max[M1, M2, \dots, Mk]$ ）。

#### 【0374】

対応する識別子が1以上抽出された場合は（ステップ13のY）、抽出された識別子を誘導部8001へ返す（ステップ15）。このとき、複数の識別子が抽出された場合は、必須信頼度が最大である識別子を1つだけ誘導部8001へ戻してもよいし、全ての識別子を戻してもよい。誘導部8001は、サーバ管理部8002から入力した識別子に対応するおとり装置2またはサーバ装置401へパケットpを転送する（ステップ16）。

#### 【0375】

サーバ装置401がパケットpを受信すると、サーバ装置401上のサーバプログラムによりパケットpの処理が行われる。一方、おとり装置2がパケットpを受信すると、すでに述べたように、プロセッサ上でサーバプログラムを動作させ、攻撃検知部でそのふるまいを監視する（ステップ17）。

#### 【0376】

そして、転送先のおとり装置 2 もしくはサーバ装置 401 上のサーバプログラムが出力したレスポンスは、誘導部 8001 を経て、パケット p の送信元ホストへと返送される（ステップ I 8）。なお、転送先であるおとり装置 2 が複数である場合、レスポンスも複数得られるが、誘導部 8001 は必須信頼度が最大であるおとり装置 2 から得られたレスポンスのみをアクセス元へ転送する。ただし、転送先にサーバ装置 401 が含まれる場合には、必ずサーバ装置 401 からのレスポンスを採用して転送する。

【0377】

#### 17. 3) 効果

上述したように、おとりサーバに必須信頼度を割り当てておき、この必須信頼度に応じて、様々な重要度をもつコンテンツの配置・非配置を決定することができる。これにより、おとりサーバ上で被害が発生した場合でも、予め想定したレベル以下に抑制することができる。

【0378】

#### （第 18 実施形態）

これまで述べてきた実施形態における信頼度管理部は、おとり装置 2 からのアラートに基づいて信頼度を調整するものであったが、本発明はこれに限定されるものではなく、外部の一般的な攻撃検知システムから攻撃検知通知に基づいて信頼度調整を行うこともできる。これにより、他のサイトで発生した攻撃事例を基に予防的な防御を行うことが可能となる。

【0379】

#### 18. 1) 構成

図 64 は、本発明の第 18 実施形態による攻撃防御システムの概略的構成図である。本実施形態における攻撃防御システムは、ファイアウォール装置 81 と、内部ネットワーク 8103 および外部ネットワーク 8104 上にある 1 つ以上の攻撃検知システム A D<sub>1</sub>～A D<sub>n</sub>と、を備える。

【0380】

ファイアウォール装置 81 は、少なくとも信頼度管理部 8101 とアラート変換部 8102 とを有する。信頼度管理部 8101 は、アラート変換部 8102 によって変換されたアラートを入力すると、すでに述べた手順により、後続する入力パケットの信頼度を減算する。なお、攻撃検知システム A D<sub>1</sub>～A D<sub>n</sub>は、それぞれのシステムに依存した構文のアラートを送信するから、攻撃検知システムごとにアラームを解釈するための解釈モジュールがアラート変換部 8102 に設けられている。

【0381】

アラート変換部 8102 は、外部ネットワーク 8104 または内部ネットワーク 8103 上にある各種攻撃検知システムからシステム依存アラートを受信し、それらのアラート構文を解釈して変換し、信頼度管理部 8101 へ出力する。

【0382】

攻撃検知システム A D<sub>1</sub>～A D<sub>n</sub>は、ネットワークトラフィックまたはサーバプログラムの動作あるいはログファイルなどを監視し、攻撃を検知した際には、少なくとも攻撃元 IP アドレスおよび攻撃対象 IP アドレスを含むアラートをファイアウォール装置 81 のアラート変換部 8102 へ送信する。

【0383】

#### 18. 2) 動作

10 図 65 は、本発明の第 18 実施形態による攻撃防御システムの動作を示すフローチャートである。まず、アラート変換部 8102 は、外部ネットワークまたは内部ネットワーク上にある各種攻撃検知システムからアラートを受信すると、当該アラートの構文を解釈する（ステップ J 1）。上述したように受信アラートは送信元の攻撃検知システムに依存した構文をもっているため、アラート変換部 8102 内に備えられた攻撃検知システムごとの解釈モジュールを適切に選択し、選択された解釈モジュールにより受信アラートの構文を解釈する。解釈モジュールの選択にあたっては、たとえば、アラートの送信元 IP アドレスを基に攻撃検知システムの種類を特定すればよい。そして、解釈結果から、少なくとも攻撃パケットの送信元 IP アドレスと宛先 IP アドレスとを抽出する（ステップ J 2）。

【0384】

20 続いて、アラート変換部 8102 は、解釈結果から、受信アラートの深刻度を算出する（ステップ J 3）。深刻度の算出方法の具体例としては、例えばアノマリ型攻撃検知システムによるアラートであれば異常さを示す数値が記載されているので、それを深刻度として採用する。また、シグネチャ型攻撃検知システムによるアラートであれば、攻撃方法を示す識別子から予め対応づけられた深刻度を求めるようにしてもよい。

【0385】

そして、少なくとも送信元 IP アドレス、宛先 IP アドレス、および、深刻度という 3 つの値を 1 組として生成し、変換済みアラートとして信頼度管理部 8101 へ出力する（ステップ J 4）。

【0386】

40 変換済みアラートを入力した信頼度管理部 8101 は、送信元 IP アドレスまたは宛先 IP アドレス、あるいは（もし取得可能であれば）攻撃データに対する信頼度から深刻度を減算することで、信頼度の更新を行う（ステップ J 5）。

【0387】

#### （第 19 実施形態）

50 第 1～第 18 実施形態におけるファイアウォール装置では、信頼度管理部を内部に有していたが、本発明はこれに限定されるものではなく、信頼度管理部を別ユニットで構成することもできる。これにより、ファイアウォ



ール装置が多数存在する場合にも、少数の信頼度管理用ユニットでファイアウォール装置の動作を制御できるようになり、運用コストが低減するというメリットがある。

#### 【0388】

##### 19. 1) 構成

図 66 は、本発明の第 19 実施形態による攻撃防御システムの概略的ブロック図である。本実施形態による攻撃防御システムは、ファイアウォール装置 85 と、信頼度管理サーバ装置 86 と、少なくとも 1 つのおとり装置 2 もしくは攻撃検知システムを備えている。ファイアウォール装置 85 は、少なくとも誘導部 8501 および管理サーバ接続部 8502 を有する。誘導部 8501 は、外部ネットワークから受信した入力 IP パケットを管理サーバ接続部 8502 へ渡して信頼度を取得し、入力 IP パケットを内部ネットワーク上のサーバ装置 401 またはおとり装置 2 へ転送する。

#### 【0389】

管理サーバ接続部 8502 は、少なくとも 1 つの信頼度管理サーバ装置 86 に接続されており、誘導部 8501 から入力した入力 IP パケットの全てまたは一部を含む信頼度要求メッセージを信頼度管理サーバ装置 86 へ送信する。信頼度管理サーバ装置 86 から信頼度を含む応答メッセージを受信すると、管理サーバ接続部 8502 は当該信頼度を誘導部 8501 へ返す。

#### 【0390】

信頼度管理サーバ 86 は、ファイアウォール装置 85 から信頼度要求メッセージを受信すると、所定の方法により算出された信頼度を含む応答メッセージを当該ファイアウォール装置 85 へ返信する。

#### 【0391】

##### 19. 2) 動作

図 67 は、本発明の第 19 実施形態による攻撃防御システムの動作を示すフローチャートである。ファイアウォール装置 85 は、まず、新たに外部ネットワークから受信した入力 IP パケットを誘導部 8501 へ転送する（ステップ K1）。

#### 【0392】

誘導部 8501 から入力 IP パケットを受け取ると、管理サーバ接続部 8502 は、当該入力 IP パケットから信頼度要求メッセージを生成し、所定の信頼度管理サーバ装置 86 へ送信する（ステップ K2）。なお、所定の信頼度管理サーバ装置 86 は、1 台とは限らず、複数であってもよい。また、信頼度要求メッセージは入力 IP パケットの全てを含むものでもよいし、ヘッダやペイロードなどの一部を含むものでもよい。信頼度要求メッセージに含めるべき情報は、信頼度管理サーバ装置 86 における信頼度の算出方法に依存するので、複数の信頼度管理サーバ装置がある場合には、各信頼度管理サーバ装置に応じて、信頼度要求メッセージのフォーマ

ットを定めるようにしてもよい。

#### 【0393】

次に、信頼度要求メッセージを受信すると、信頼度管理サーバ装置 86 は、当該信頼度要求メッセージに含まれる入力 IP パケットの全てまたは一部を抽出し（ステップ K3）、当該入力 IP パケットに対する信頼度  $r$  [p] を算出する（ステップ K4）。なお、信頼度算出方法は、すでに説明した信頼度管理部の動作など信頼度としての数値を算出するものであれば任意の方法を用いてよい。あるいは、そうした信頼度管理手段を、信頼度管理モジュールとしてモジュール化しておき、動的に変更可能なようにしてもよい。こうすることにより、いわゆる「プラグイン機能」や「アップデート機能」を提供することができ、信頼度管理サーバ装置の保守性を向上させることができる。

#### 【0394】

続いて、信頼度管理サーバ装置 86 は、信頼度  $r$  [p] を含む応答メッセージを管理サーバ接続部 8502 へ送信する（ステップ K5）。なお、応答メッセージは、少なくとも信頼度を数値として含むものであれば、ほかにどのような情報が付加されていてもよい。そして、応答メッセージを受信した管理サーバ接続部 8502 は、当該応答メッセージから信頼度を抽出した後、当該信頼度を誘導部 8501 へ出力する（ステップ K16）。

#### 【0395】

なお、複数の信頼度管理サーバ装置 86 から応答メッセージを受信した場合には、管理サーバ接続部 8502 で所定の関数 H により、1 つの信頼度にまとめあげた上で、誘導部 8501 へ出力する。関数 H の具体例としては、複数の信頼度のうち最小のものを返す関数あるいは平均値を返す関数などを用いることができる。

#### 【0396】

信頼度を受け取った誘導部 8501 は、当該信頼度と所定の振り分け条件とを照合した結果に基づいて、入力 IP パケットをサーバ装置 401 およびおとり装置 2 のいずれかへと転送する（ステップ K7）。

#### 【図面の簡単な説明】

#### 【0397】

【図 1】本発明による攻撃防御システムの概略的ブロック図である。

【図 2】本発明の第 1 実施形態による攻撃防御システムのファイアウォール装置 1 およびおとり装置 2 の構成を示すブロック図である。

【図 3】図 2 のファイアウォール装置 1 におけるアクセス制御リスト管理部 102 の模式的構成図である。

【図 4】アクセス制御リストデータベース 1021 の内容を例示した模式図である。

【図 5】誘導部 103 に設けられた誘導リストの一例を示す模式図である。

【図 6】防御ルール判定部 107 に保持されているアク

セス制御ルールのひな型を例示した模式図である。

【図 7】本発明の第 1 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 8】本発明の第 1 実施形態のファイアウォール装置でアドレス変換処理を行う際の好適な一例を示すブロック図である。

【図 9】第 1 実施形態の具体的な動作例を説明するためのネットワーク構成図である。

【図 10】第 1 実施形態の具体的な動作例を説明するためのネットワーク構成図である。

【図 11】第 1 実施形態の具体的な動作例を説明するためのネットワーク構成図である。

【図 12】おとり装置 2 における攻撃検知動作を説明するための模式図である。

【図 13】第 1 実施形態におけるアクセス制御リストの更新動作例を説明するための模式図である。

【図 14】第 1 実施形態の具体的な動作例を説明するためのネットワーク構成図である。

【図 15】本発明の第 2 実施形態による攻撃防御システムのブロック図である。

【図 16】本発明の第 2 実施形態による攻撃防御システムの動作を示すフローチャートである。

【図 17】本実施形態における信頼度とパケット転送先の関係を示すグラフである。

【図 18】(A) は、外れ値度計算を用いた信頼度管理部 502 の概略的構成図であり、(B) は、その一例を示す詳細なブロック図である。

【図 19】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 20】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 21】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図 22】本発明の第 3 実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図である。

【図 23】第 3 実施形態による攻撃防御システムのファイアウォール装置の一例を示す詳細なブロック図である。

【図 24】本発明における第 4 実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。

【図 25】信頼度管理部 701 における信頼度参照処理を示すフローチャートである。

【図 26】本発明の第 6 実施形態による攻撃防御システムのファイアウォール装置 9 を示す概略的ブロック図である。

【図 27】本実施形態によるファイアウォール装置 9 の動作を示すフローチャートである。

【図 28】本発明の第 7 実施形態による攻撃防御システ

ムのファイアウォール装置 10 を示す概略的ブロック図である。

【図 29】アクセス制御リスト管理部 1002 の管理動作を示すフローチャートである。

【図 30】本発明の第 8 実施形態による攻撃防御システムの概略的構成図である。

【図 31】本発明の第 10 実施形態による攻撃防御システムの概略的構成図である。

【図 32】本発明の第 11 実施形態による攻撃防御ユニットの概略的構成図である。

【図 33】本発明の第 12 実施形態におけるおとり装置の構成を示すブロック図である。

【図 34】第 12 実施形態におけるおとり装置の全体的動作を示すフローチャートである。

【図 35】第 12 実施形態において使用されるプロセス種別判定テーブルの一例を示す図である。

【図 36】イベント管理部におけるイベント管理キューの一例を示す図である。

【図 37】第 12 実施形態におけるイベント管理部が行うリンク付け処理の 1 例を示すフローチャートである。

【図 38】第 12 実施形態におけるイベント管理部が出力するイベントーコンテキスト対の概念図である。

【図 39】ドメインタイプ制約つき正常動作定義 (D T 定義) ファイルの一例を示す図である。

【図 40】第 12 実施形態における攻撃検知部が解釈するドメインタイプ制約の概念図である。

【図 41】第 12 実施形態におけるおとり装置のイベント管理部が行うネットワークイベント追加の具体例を示す模式図である。

【図 42】第 12 実施形態におけるおとり装置のイベント管理部が行うプロセスイベント走査の具体例を示す模式図である。

【図 43】第 12 実施形態におけるおとり装置のイベント管理部が行うリンク付けの具体例を示す模式図である。

【図 44】第 12 実施形態におけるおとり装置のイベント管理部が行う子プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。

【図 45】第 12 実施形態におけるおとり装置のイベント管理部が行う子プロセスが発生させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。

【図 46】第 12 実施形態におけるおとり装置のイベント管理部が行う孫プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。

【図 47】第 12 実施形態におけるおとり装置のイベント管理部が行う孫プロセスが発生させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。

【図 48】第 12 実施形態のおとり装置における攻撃発

生時のイベント管理キュー状態を示す具体例を示す模式図である。

【図49】第12実施形態のおとり装置における攻撃発生時のイベント管理キュー状態を示す別の具体例を示す模式図である。

【図50】本発明の第13実施形態におけるファイアウォール装置の構成を示すブロック図である。

【図51】第13実施形態におけるファイアウォール装置の仮想サーバ部の詳細なブロック図である。

【図52】第13実施形態におけるファイアウォール装置の動作を示すフローチャートである。

【図53】第13実施形態におけるファイアウォール装置の信頼度管理部に格納される信頼度管理テーブルの一例を示す図である。

【図54】第13実施形態におけるファイアウォール装置の動作を説明するための攻撃防御システムの概略的ブロック図である。

【図55】第13実施形態における信頼度管理部が行う信頼度管理テーブルへの新規エントリ追加の具体例を示す図である。

【図56】第13実施形態におけるファイアウォール装置が行う正常動作確認時の動作の具体例を示す図である。

【図57】第13実施形態におけるファイアウォール装置が行う、攻撃検知時の動作の具体例を示す図である。

【図58】本発明の第14実施形態による攻撃防御システムの概略的ブロック図である。

【図59】本発明の第15実施形態におけるファイアウォール装置の概略的ブロック図である。

【図60】本発明の第16実施形態による攻撃防御システムの概略的構成図である。

【図61】本発明の第17実施形態による攻撃防御システムの概略的構成図である。

【図62】サーバ管理部8002が有する参照表8003の一例を示す模式図である。

【図63】本発明の第17実施形態による攻撃防御システムの動作を示すフローチャートである。

【図64】本発明の第18実施形態による攻撃防御システムの概略的構成図である。

【図65】本発明の第18実施形態による攻撃防御システムの動作を示すフローチャートである。

【図66】本発明の第19実施形態による攻撃防御システムの概略的ブロック図である。

【図67】本発明の第19実施形態による攻撃防御システムの動作を示すフローチャートである。

【符号の説明】

【0398】

1 ファイアウォール装置

100 外部通信インタフェース

101 パケットフィルタ

102 第1のアクセス制御リスト管理部

1021 アクセス制御リストデータベース

1022 検索処理部

1023 更新処理部

103 誘導部

1031 アドレス変換部

104 第1の内部通信インタフェース

105 第2の内部通信インタフェース

106 制御インタフェース

107 防御ルール判定部

2 おとり装置

21 おとりクラス

201 プロセッサ

2011 ファイルシステム

202 攻撃検知部

3 インターネット

301 攻撃元ホスト

302 通常のホスト

4 内部ネットワーク

401 サーバ装置

5 ファイアウォール装置

501 誘導部

502 信頼度管理部

5021 外れ値検知部

6 ファイアウォール装置

7 ファイアウォール装置

701 信頼度管理部

7011 リアルタイム信頼度データベース

7012 複製処理部

7013 長期信頼度データベース

7014 更新処理部

8 ファイアウォール装置

9 ファイアウォール装置

901 誘導部

9011 バッファ

9012 ICMP監視部

10 ファイアウォール装置

1001 防御ルール判定部

1002 アクセス制御リスト管理部

21 おとりクラス

37 第2のおとり装置

3701 イベント管理部

3702 第2の攻撃検知部

4101 ドメインタイプ制約つき正常動作定義ファイル

3501 第1のイベント

3601 第2のイベント

3801 第3のイベント

3901 第4のイベント

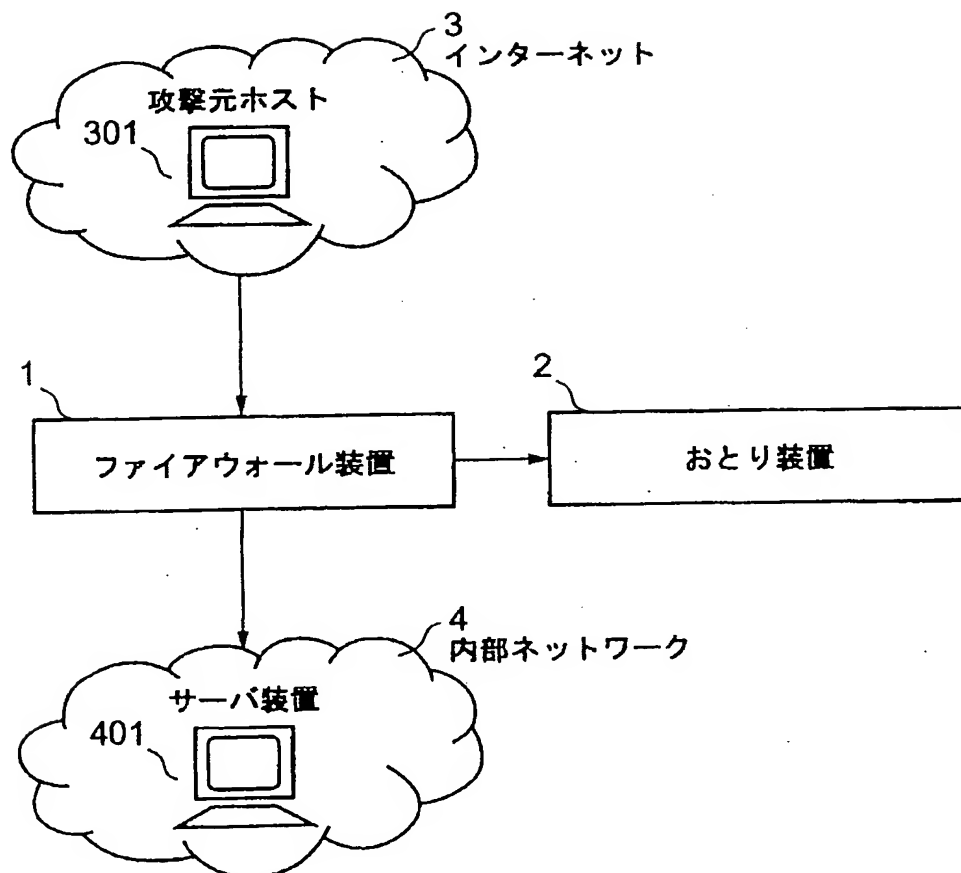
4001 第5のイベント

91  
 4101 第6のイベント  
 4901 第7のイベント  
 5001 第8のイベント  
 51 第8のファイアウォール装置  
 5101 仮想サーバ部  
 5102 第3の信頼度管理部  
 5201 接続管理部  
 5202 第1入力バッファ  
 5203 第1出力バッファ  
 5204 第2入力バッファ  
 5205 第2出力バッファ  
 62 第9のファイアウォール装置  
 6201 暗号処理部  
 303 FTPクライアント  
 402 FTPサーバ

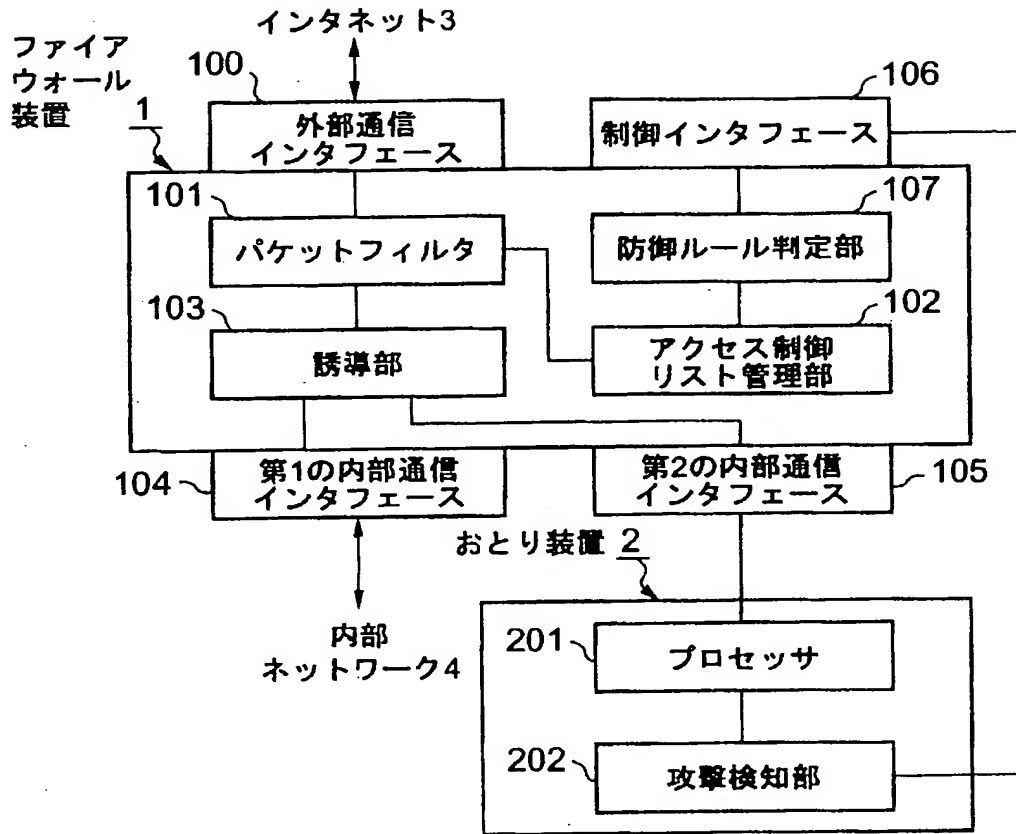
10

92  
 4021 ファイルシステム  
 6901 ミラーリング装置  
 7001 ファイアウォール装置  
 7002 スイッチ装置  
 80 ファイアウォール装置  
 8001 誘導部  
 8002 サーバ管理部  
 8003 参照表  
 81 ファイアウォール装置  
 8101 信頼度管理部  
 8102 アラート変換部  
 8501 誘導部  
 8502 管理サーバ接続部  
 86 信頼度管理サーバ装置

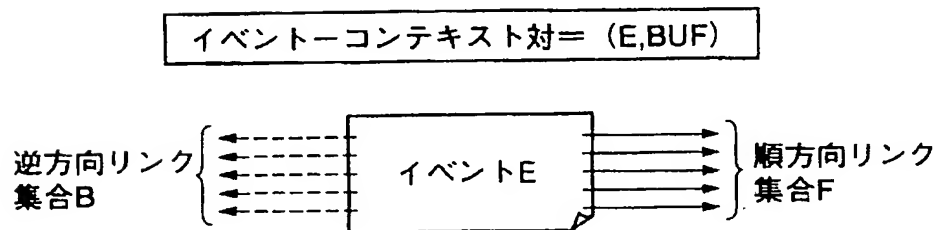
【図1】



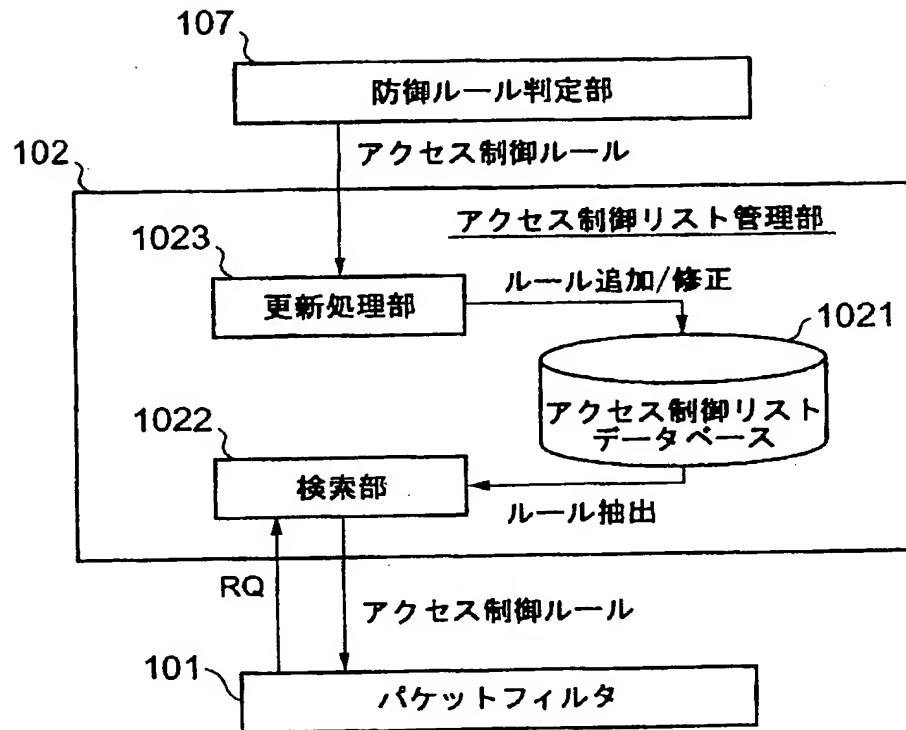
【図2】



【図38】



【図3】



【図4】

1021

アクセス制御リストデータベース		
ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

\*…任意のアドレスにマッチ

ACCEPT…パケットの受理

DENY…パケットの拒否(ICMPエラーを通知)

DROP…パケットの廃棄(ICMPエラーを通知しない)

【図5】

## 誘導リスト

1.2.3.1  
1.2.3.2  
1.2.3.3

1.2.3.5  
1.2.3.6

⋮



【図6】

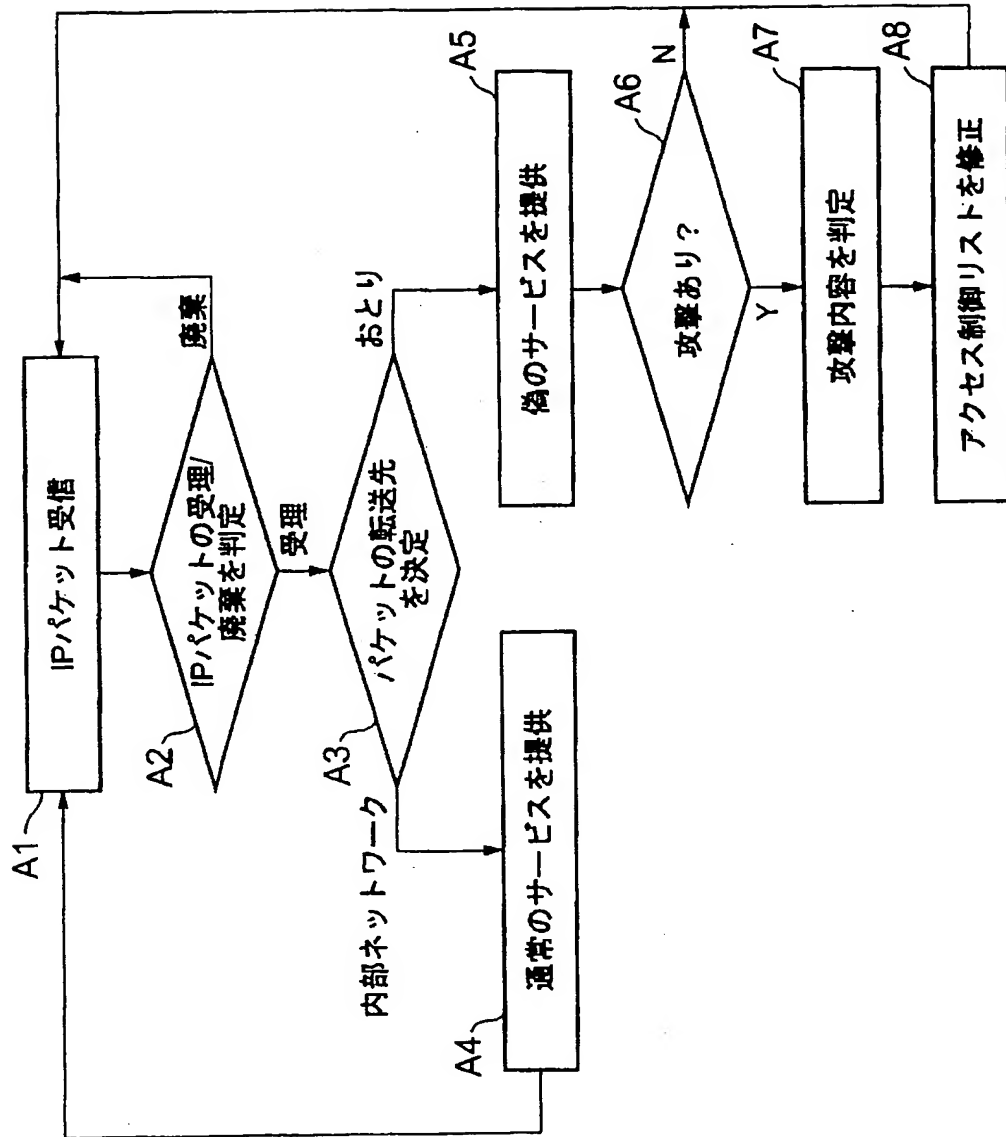
107 }

防御ルール判定部			
攻撃種別	ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
RECON	—	—	—
INTRUSION	\${SRC_IP_ADDRESS}	*	DROP
DESTRUCTION	\${SRC_IP_ADDRESS}	*	DROP

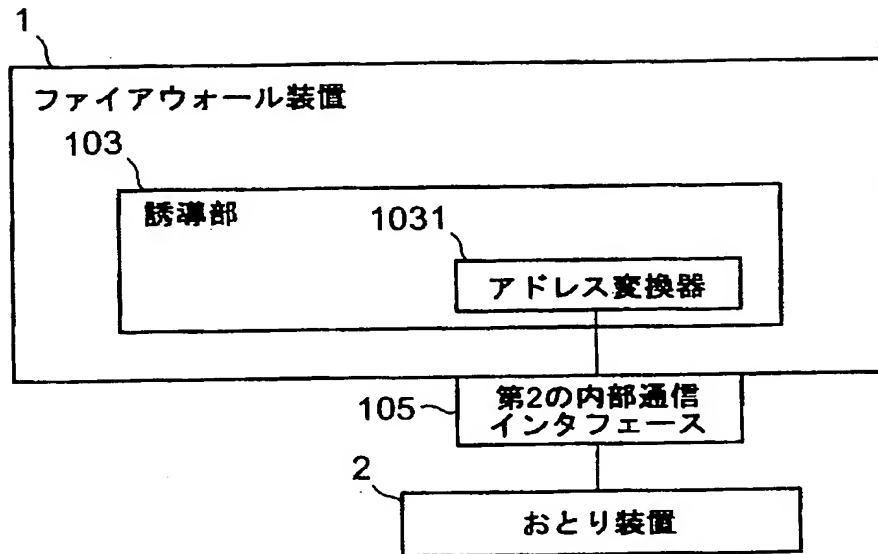
—…無指定(何もしない)

\${ }…置換用変数

【図7】

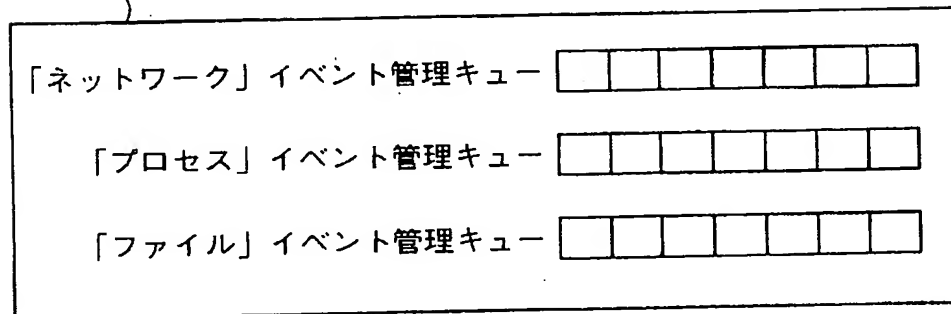


【図8】

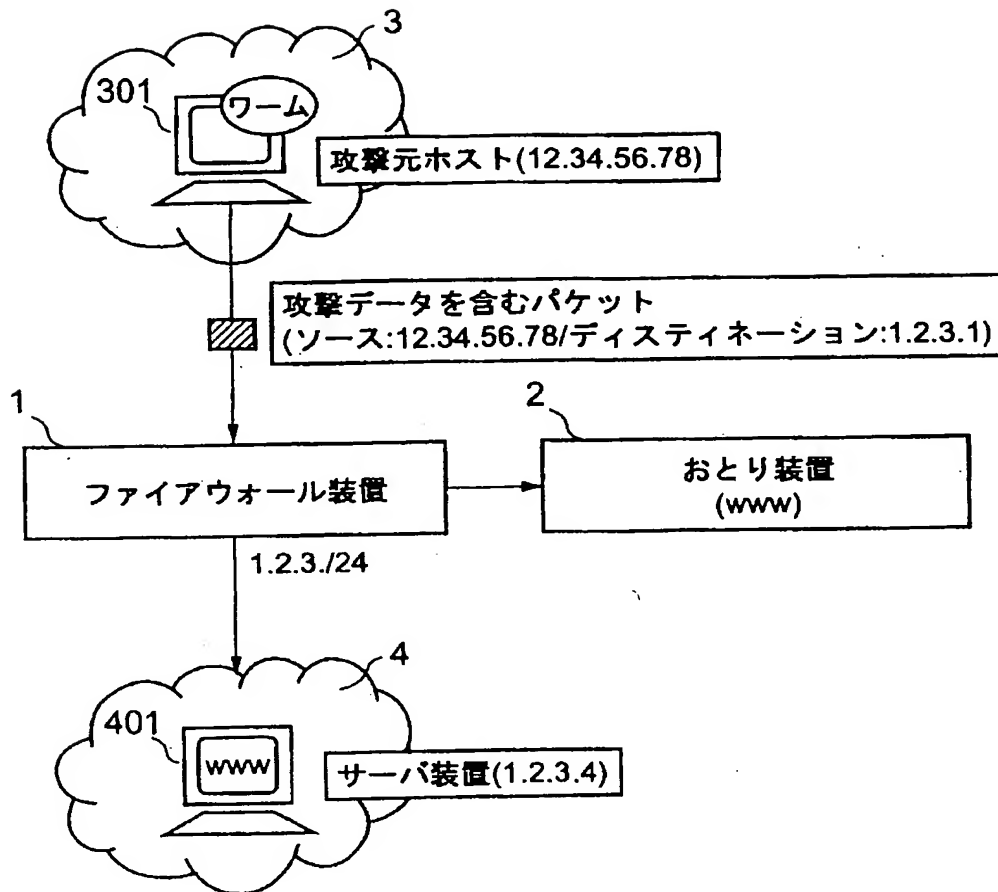


【図36】

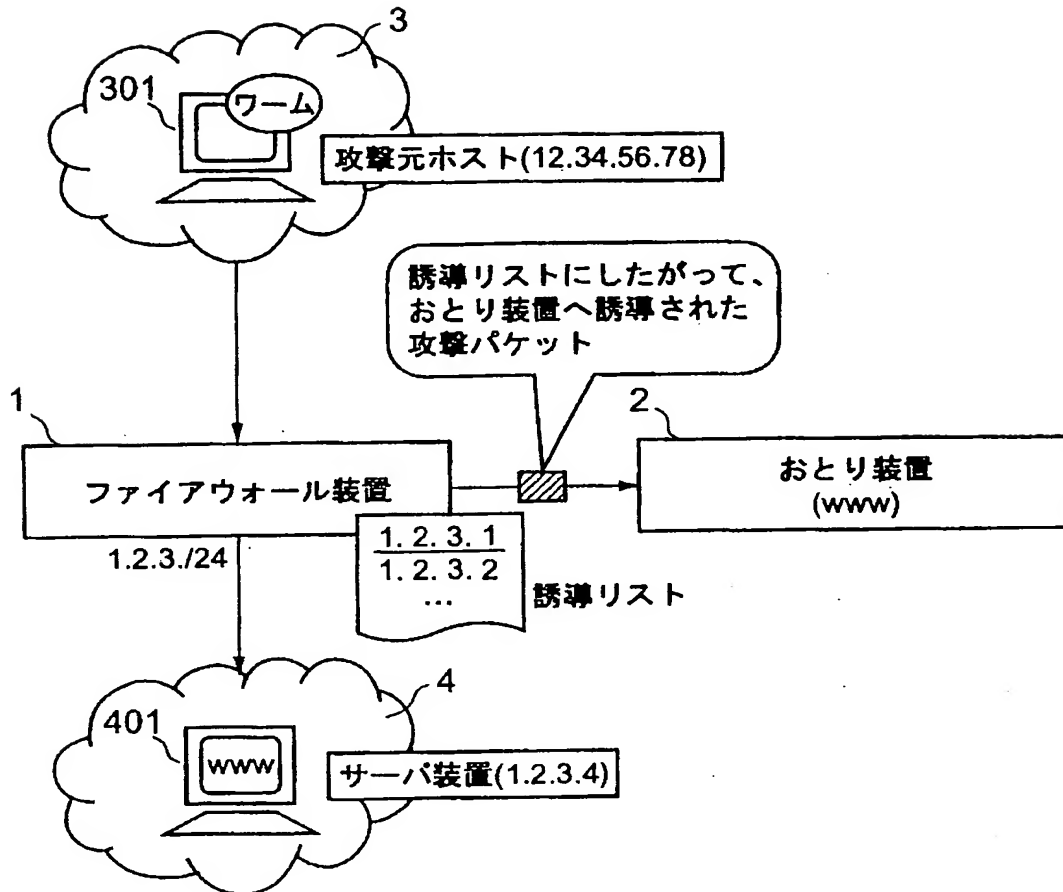
イベント管理部  
3701



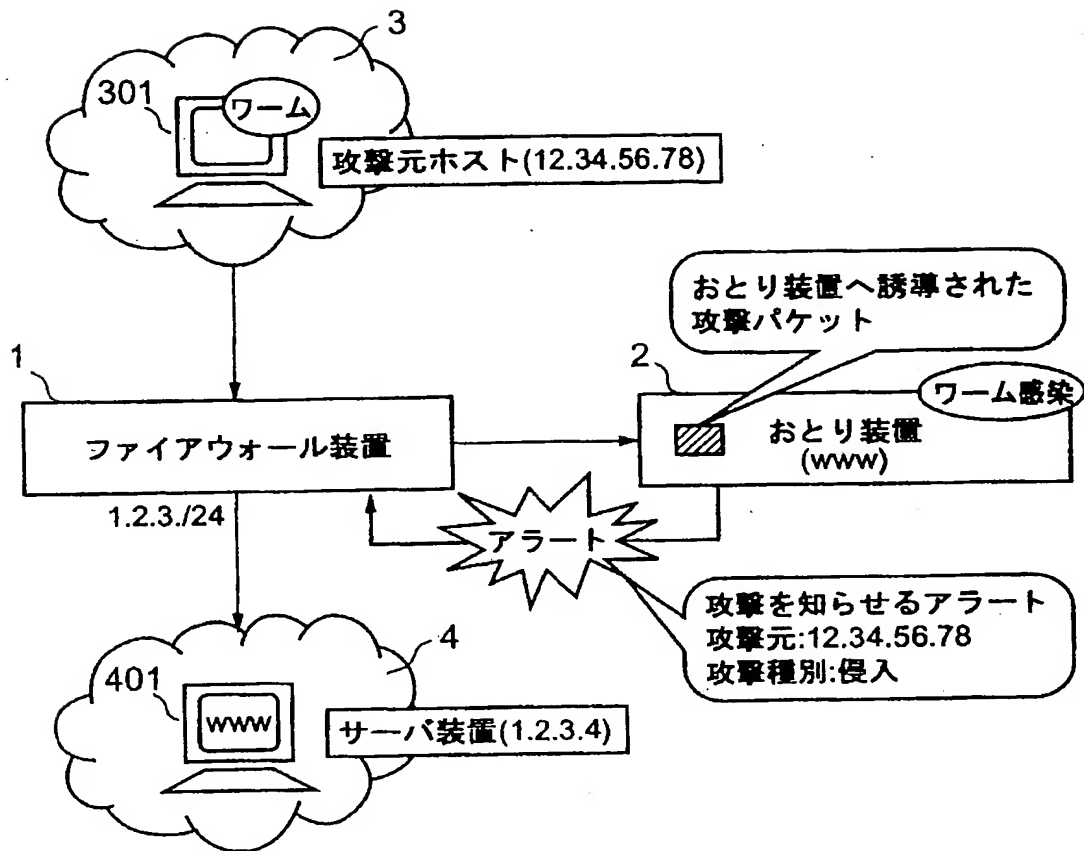
【図9】



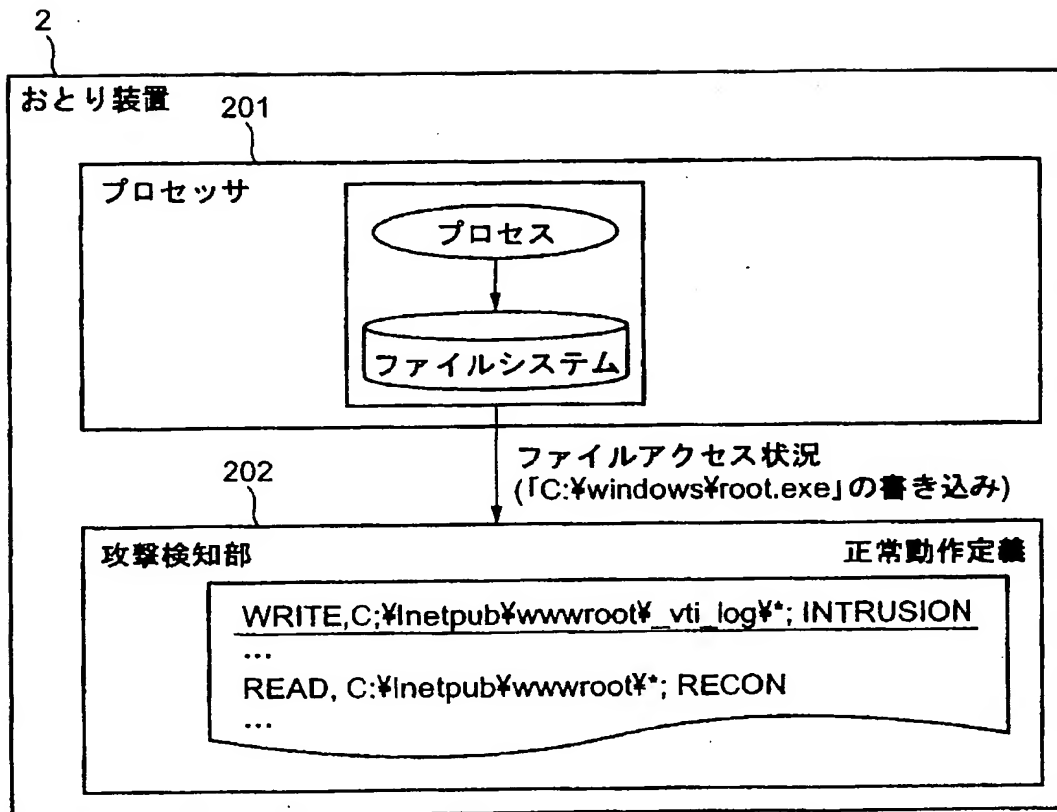
【図10】



【図11】



【図12】





【図13】

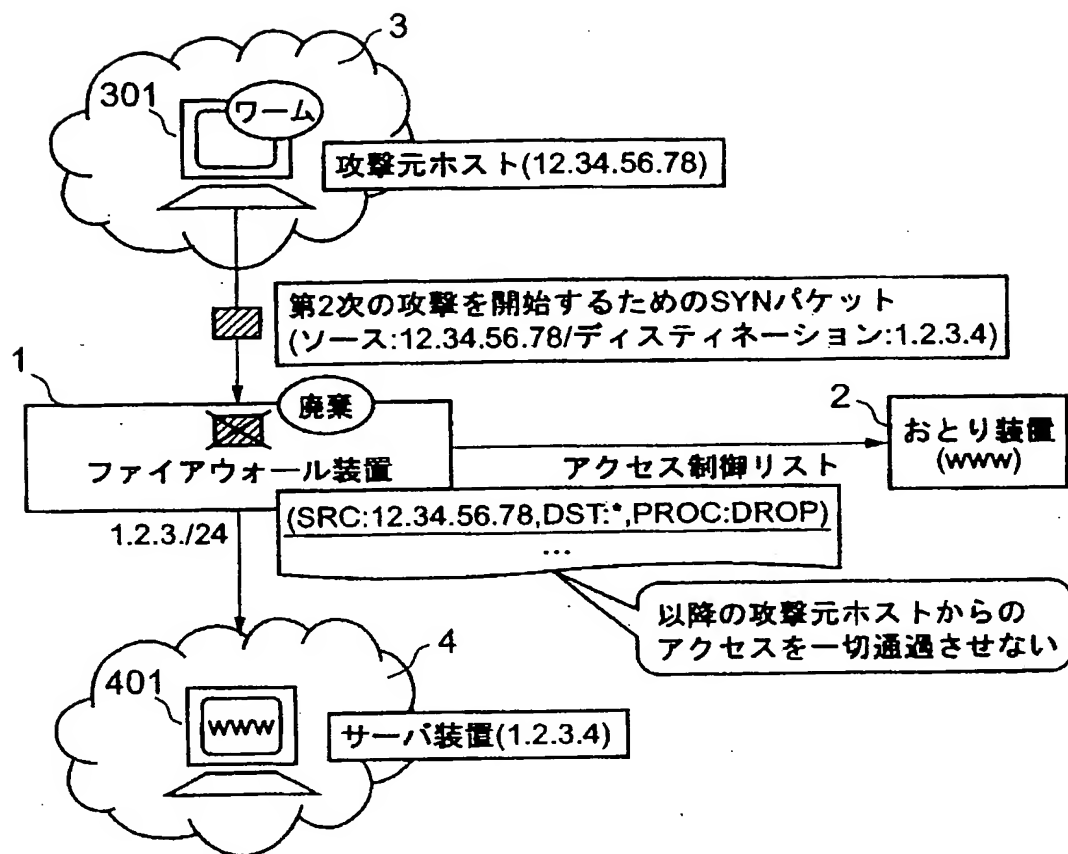
## アクセス制御リストの更新

ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

追加



【図14】



ファイアウォール装置 5

インターネット3

100 外部通信インタフェース

106 制御インタフェース

101 パケットフィルタ

107 防衛ルール判定部

102 アクセス制御リスト管理部

501 誘導部

502 信頼度管理部

104 第1の内部通信インタフェース

105 第2の内部通信インタフェース

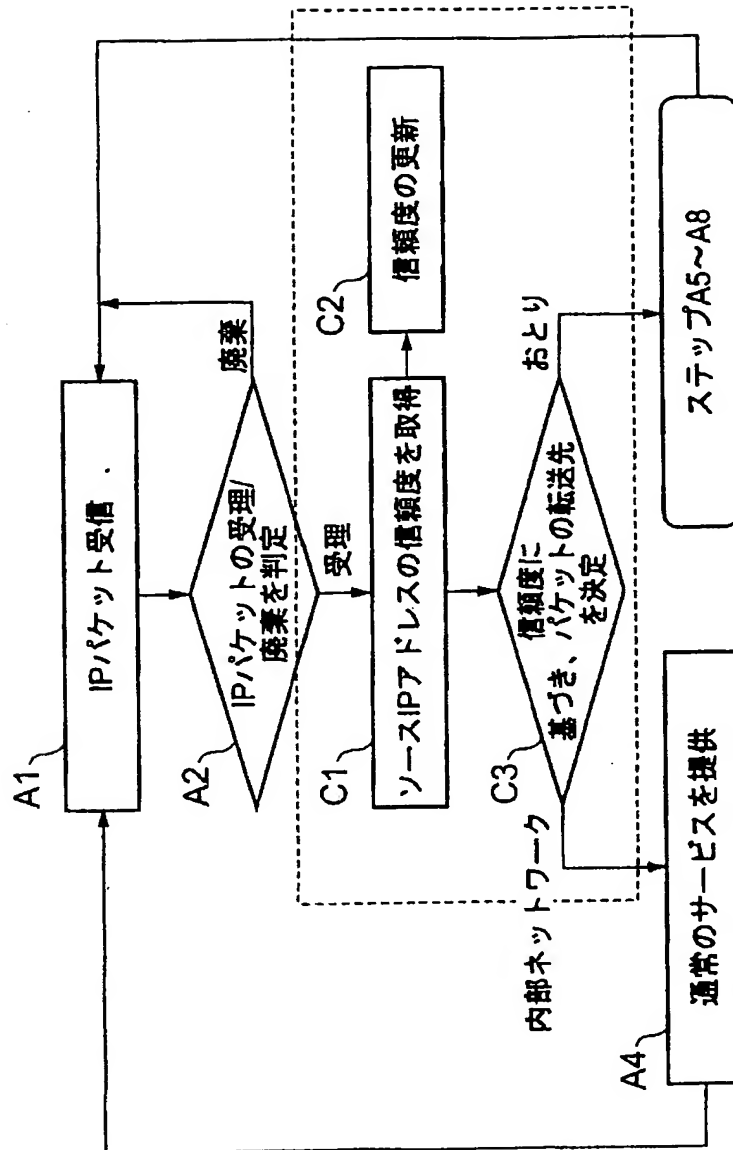
内部ネットワーク4

おとり装置 2

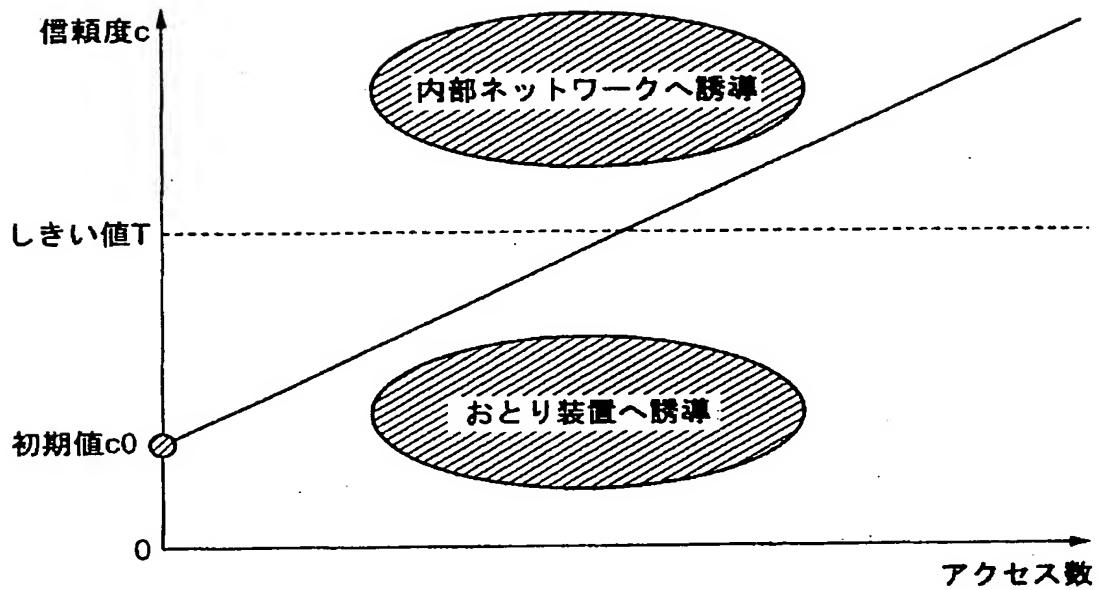
201 プロセッサ

202 攻撃検知部

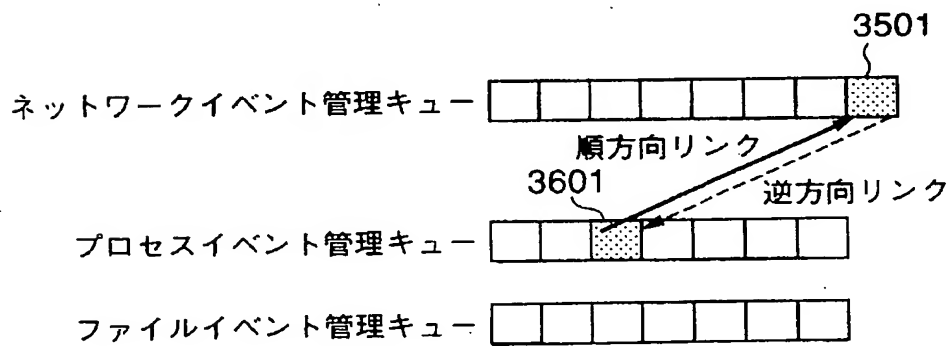
【図16】



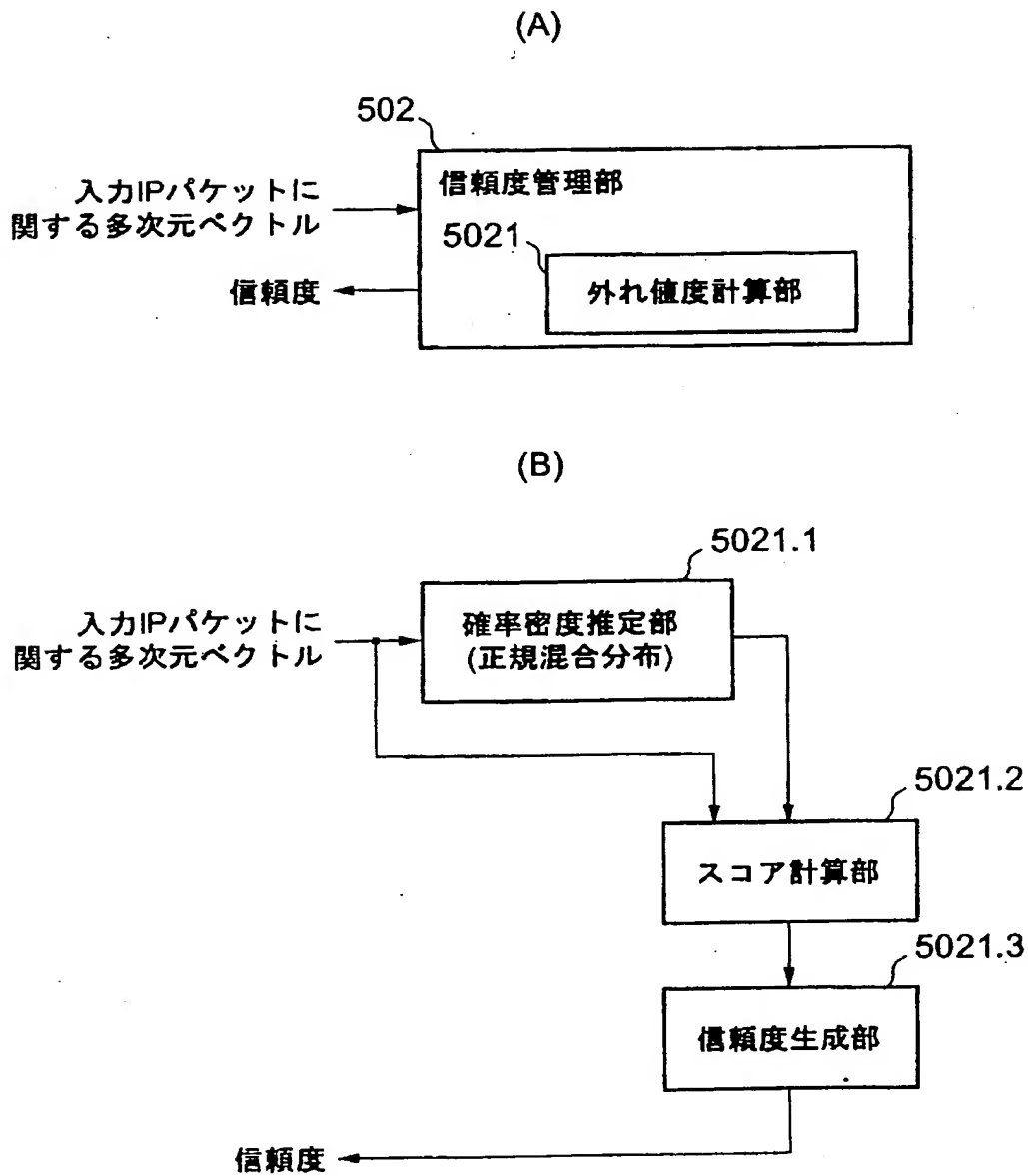
【図17】



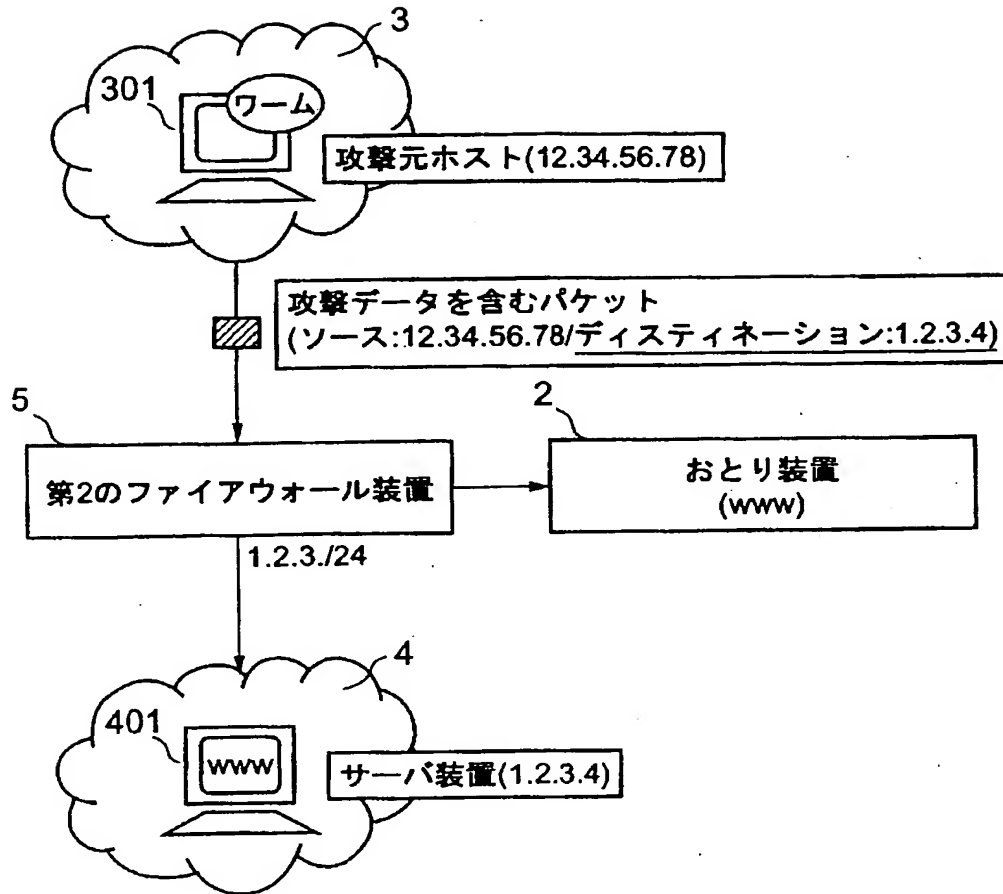
【図43】



【図18】

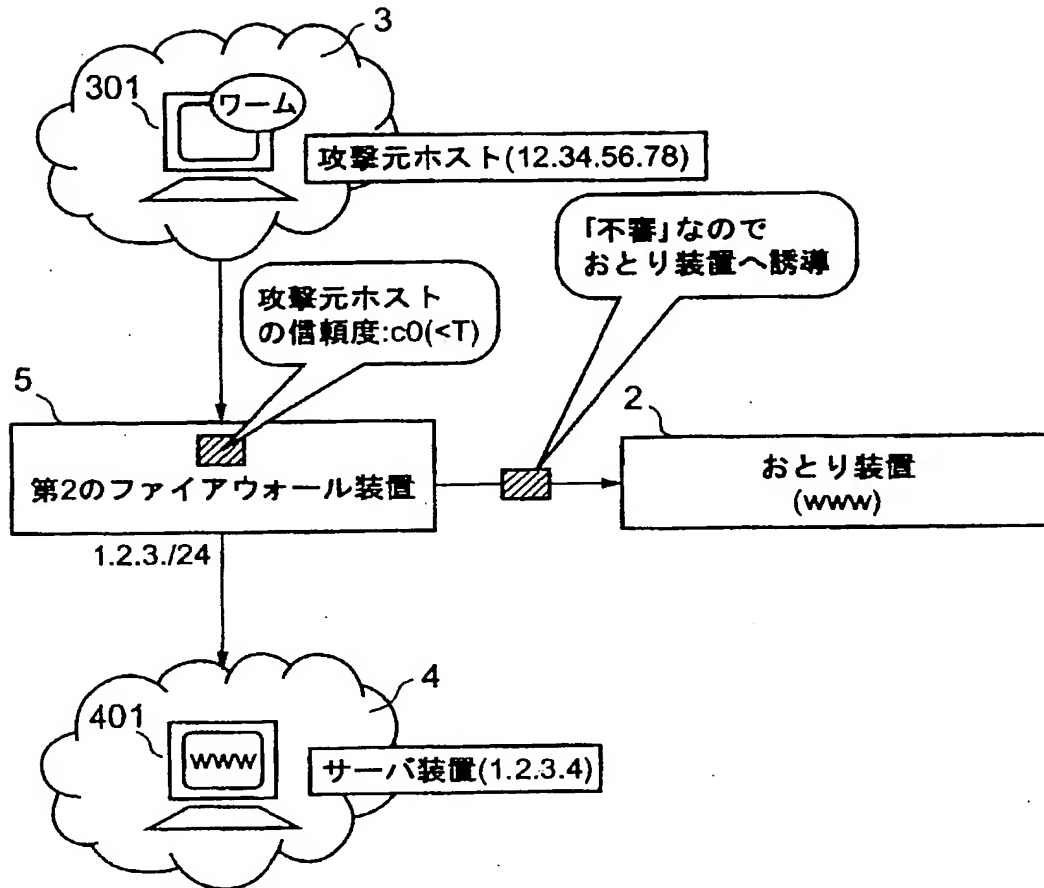


【図19】

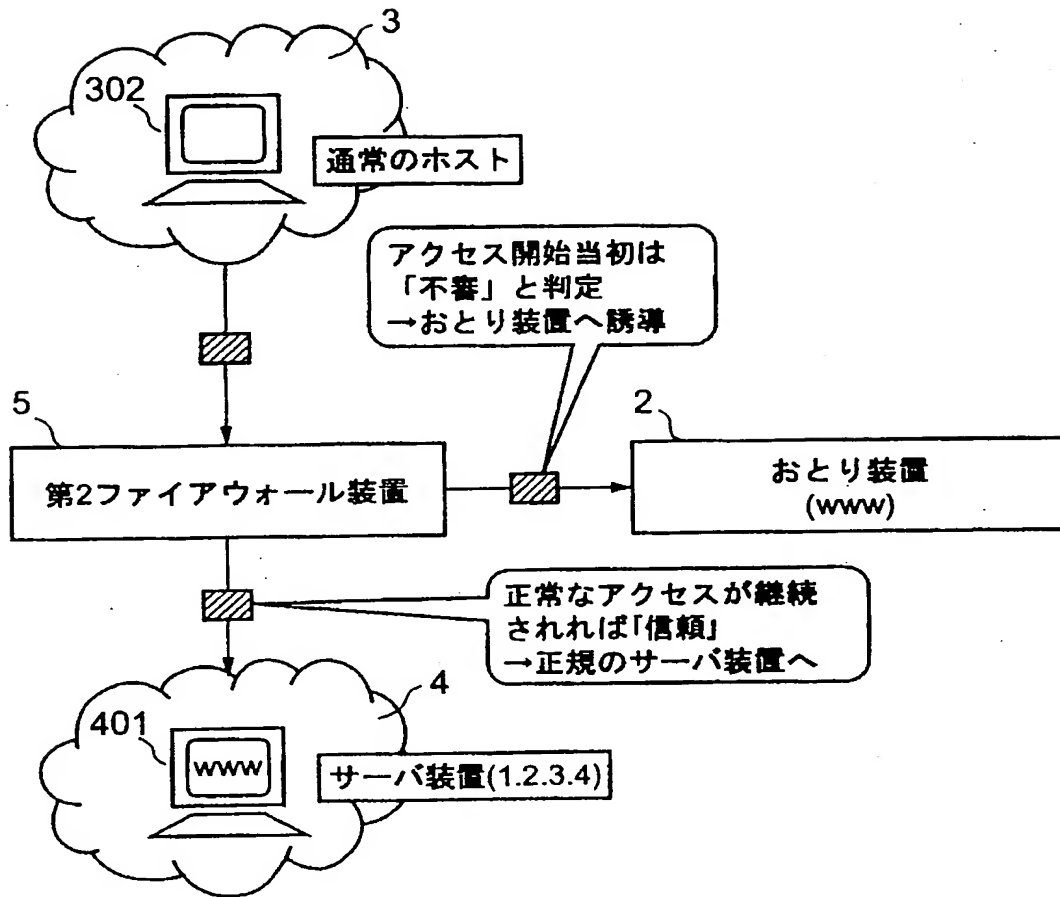




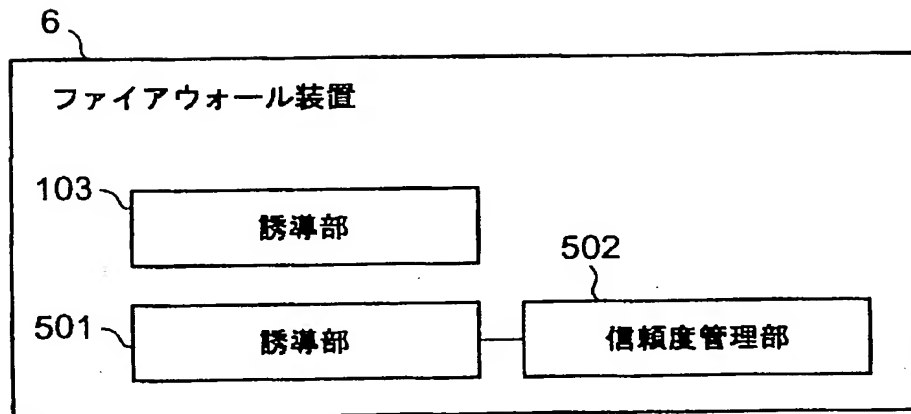
【図20】



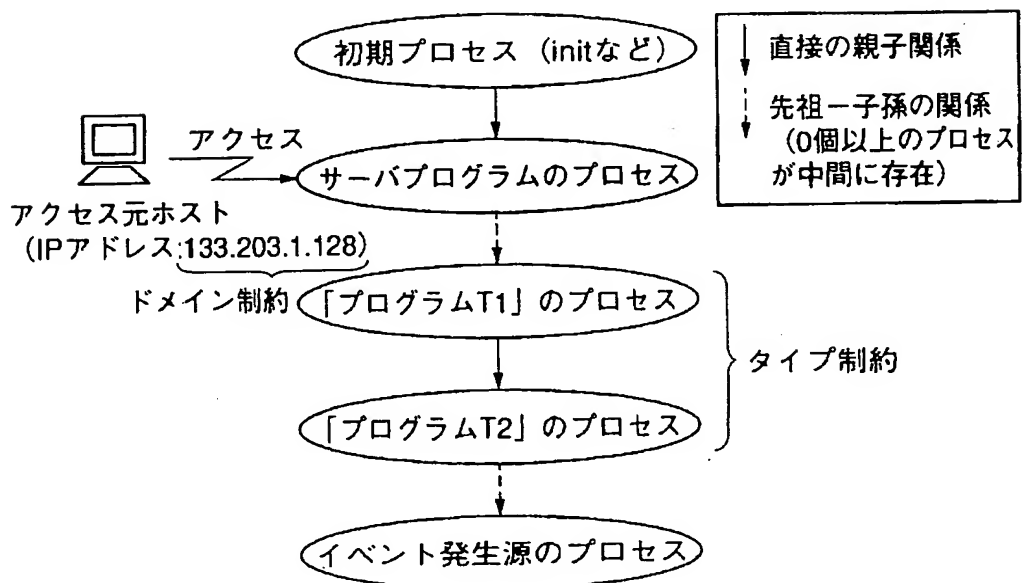
【図21】



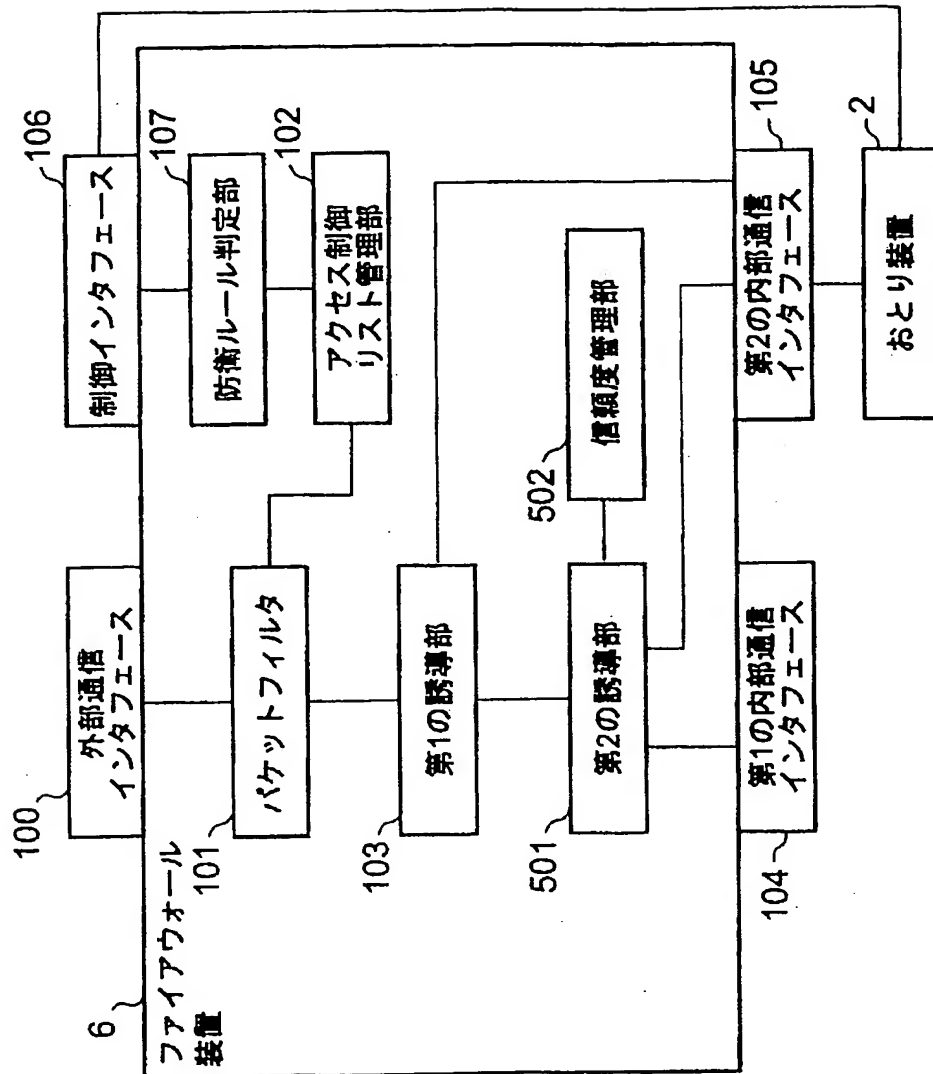
【図22】



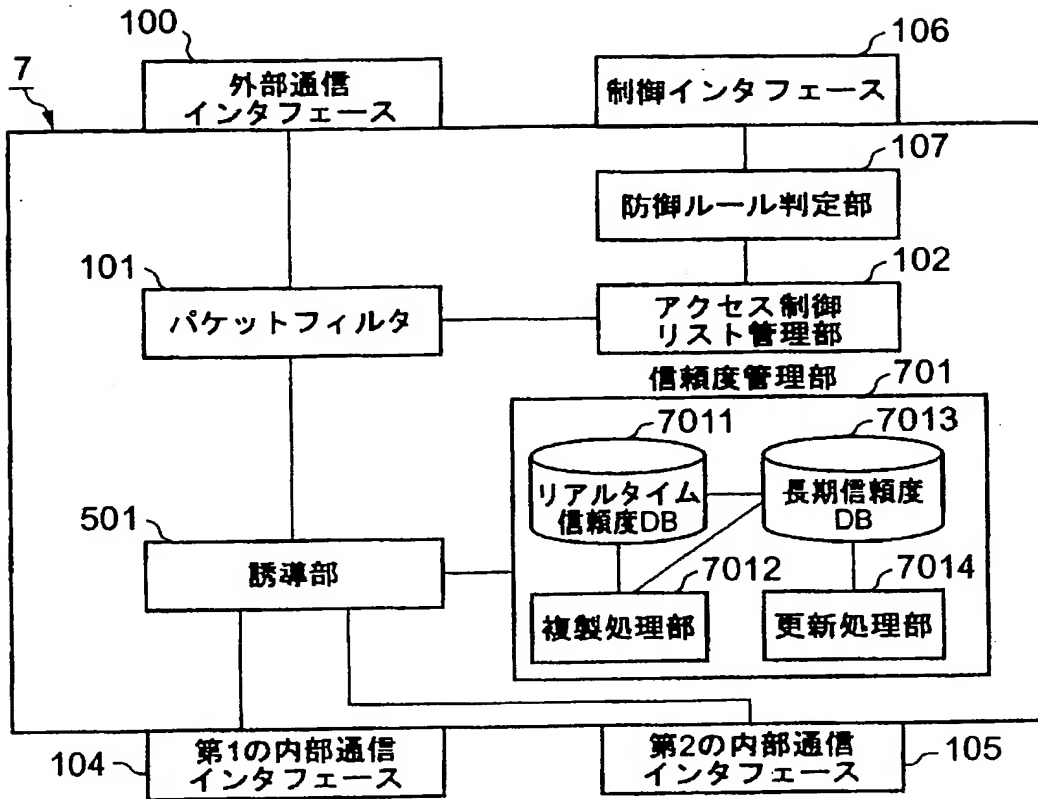
【図40】



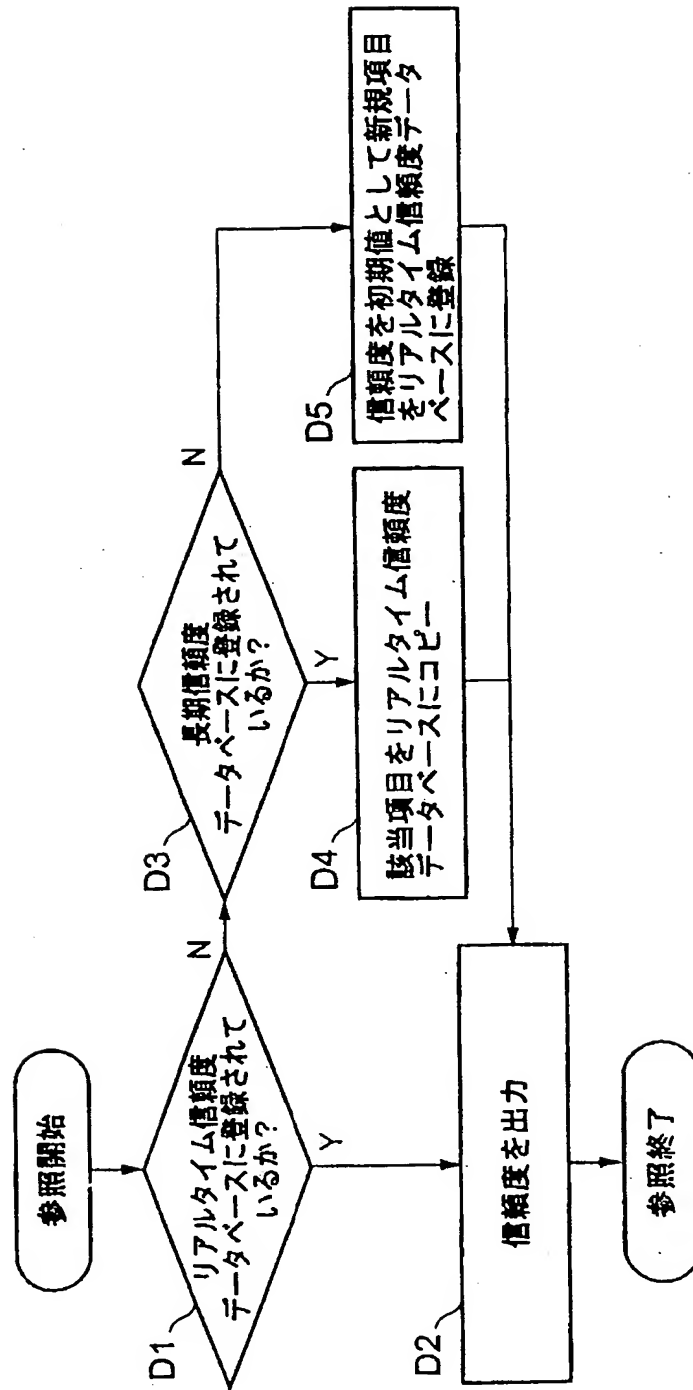
【図23】



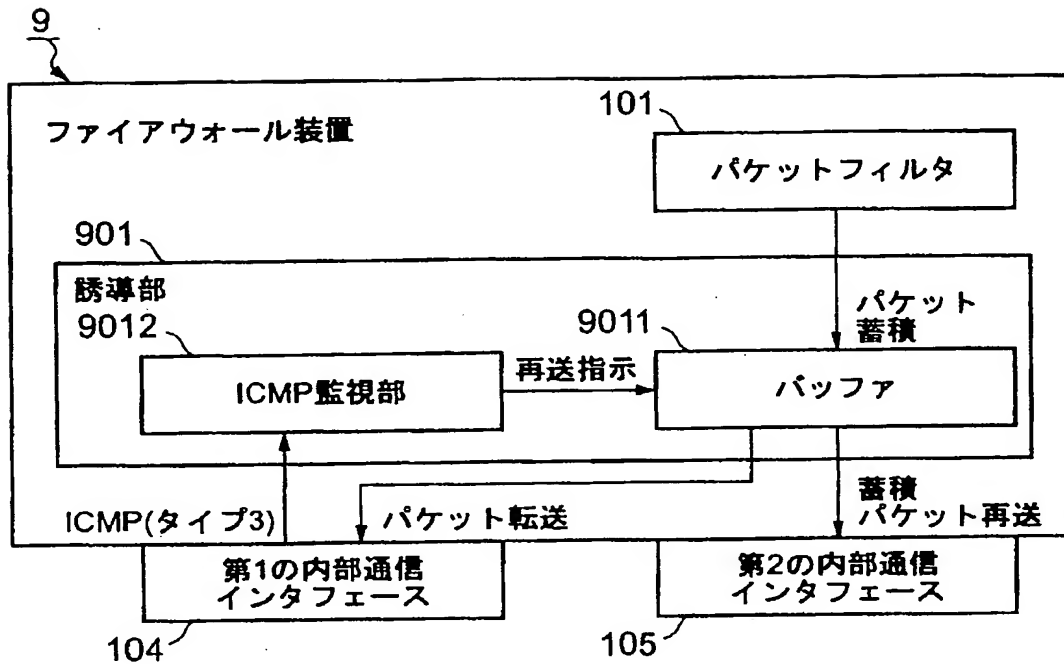
【図24】



【図25】



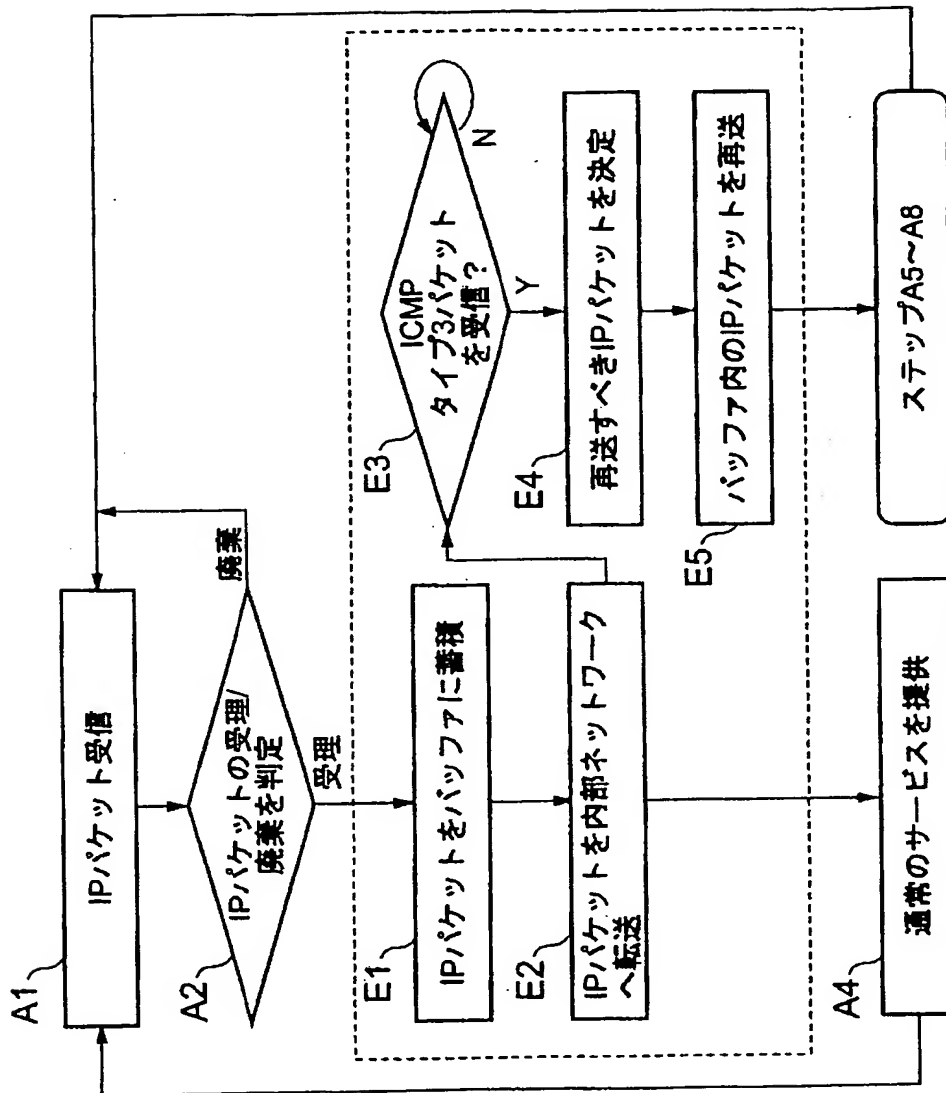
【図26】



【図55】

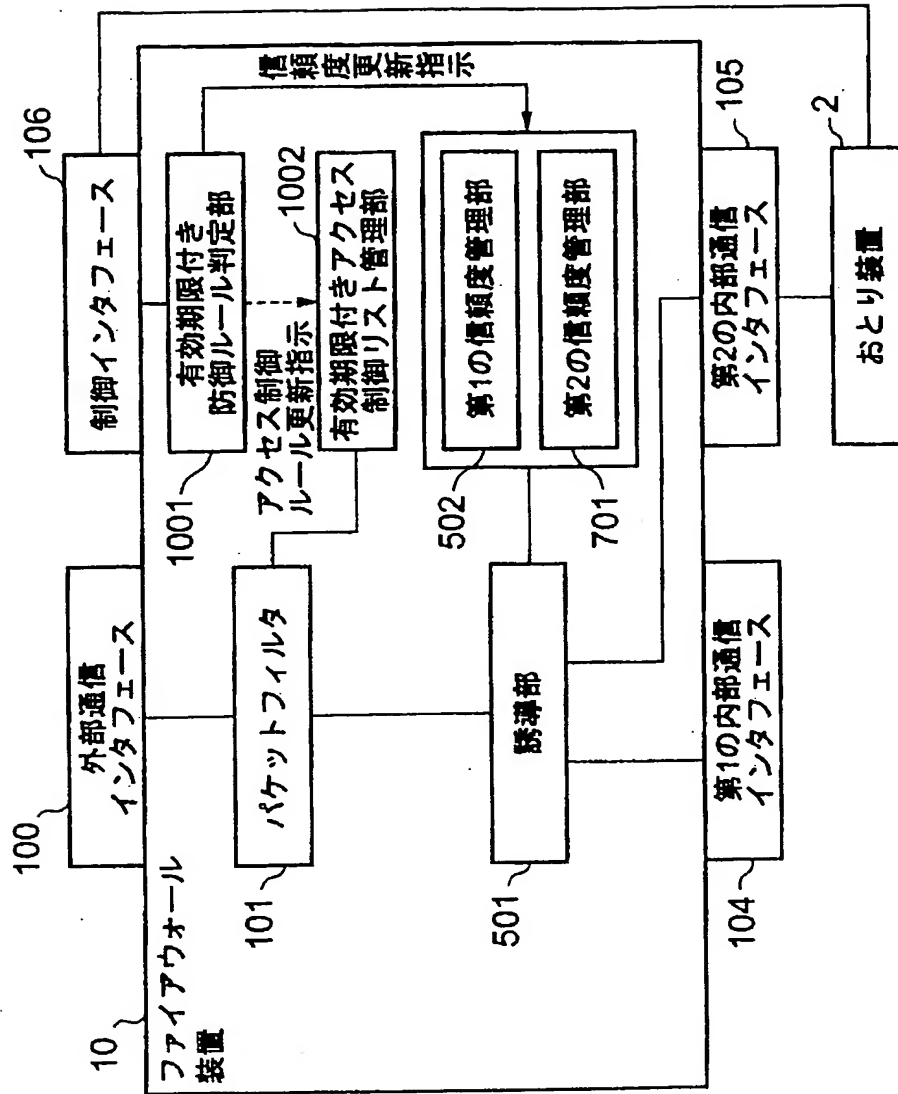
要求データ	信頼度
D0	1
D1	0
...	...
1	0

【図27】

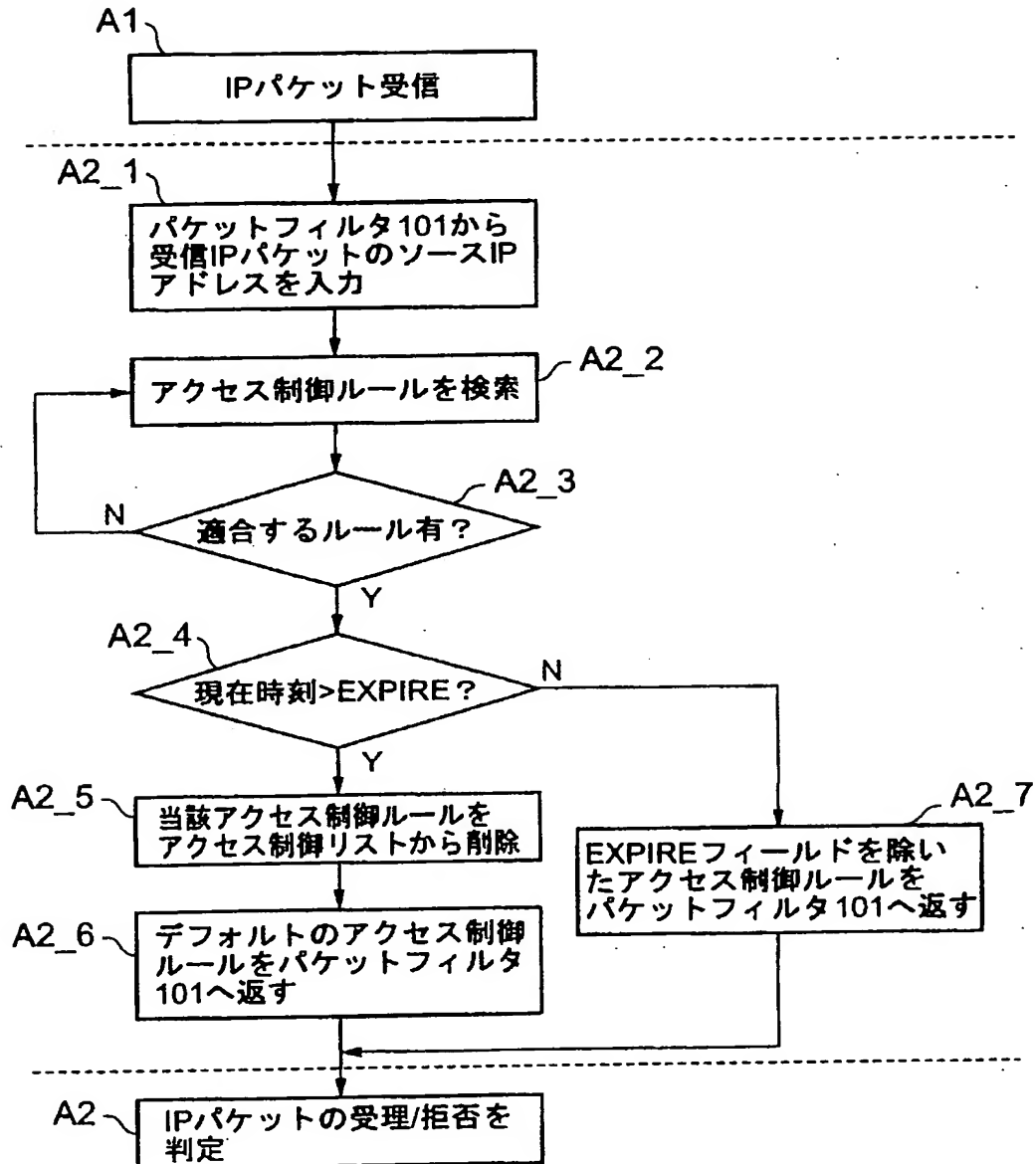




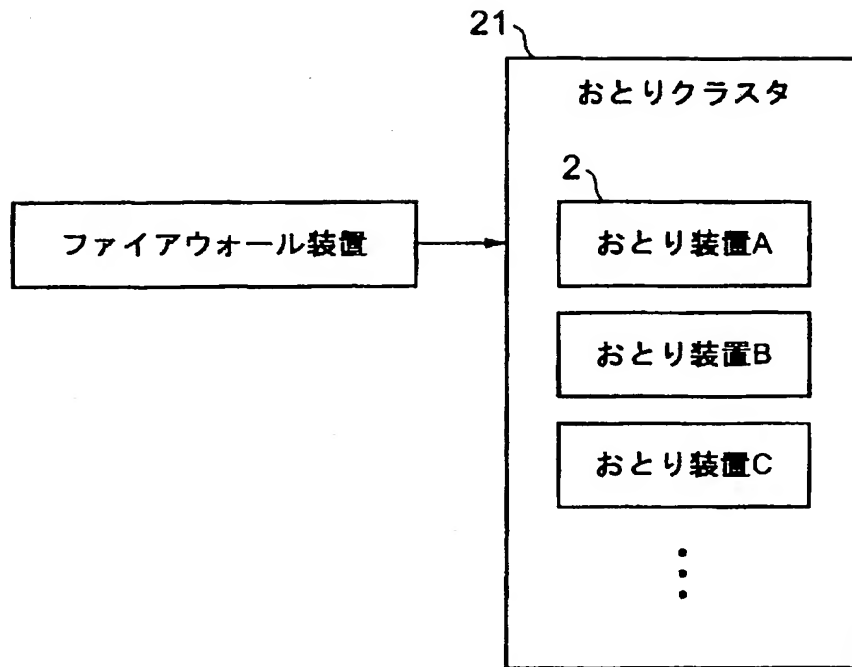
【図28】



【図29】



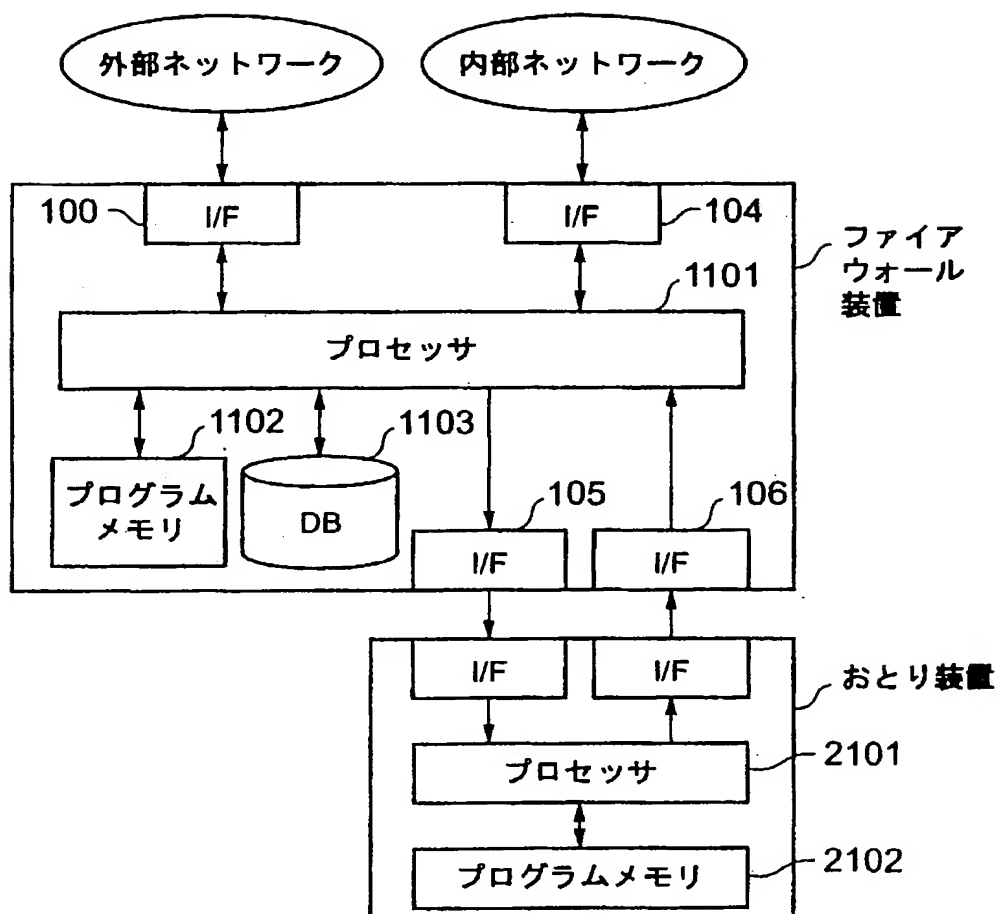
【図30】



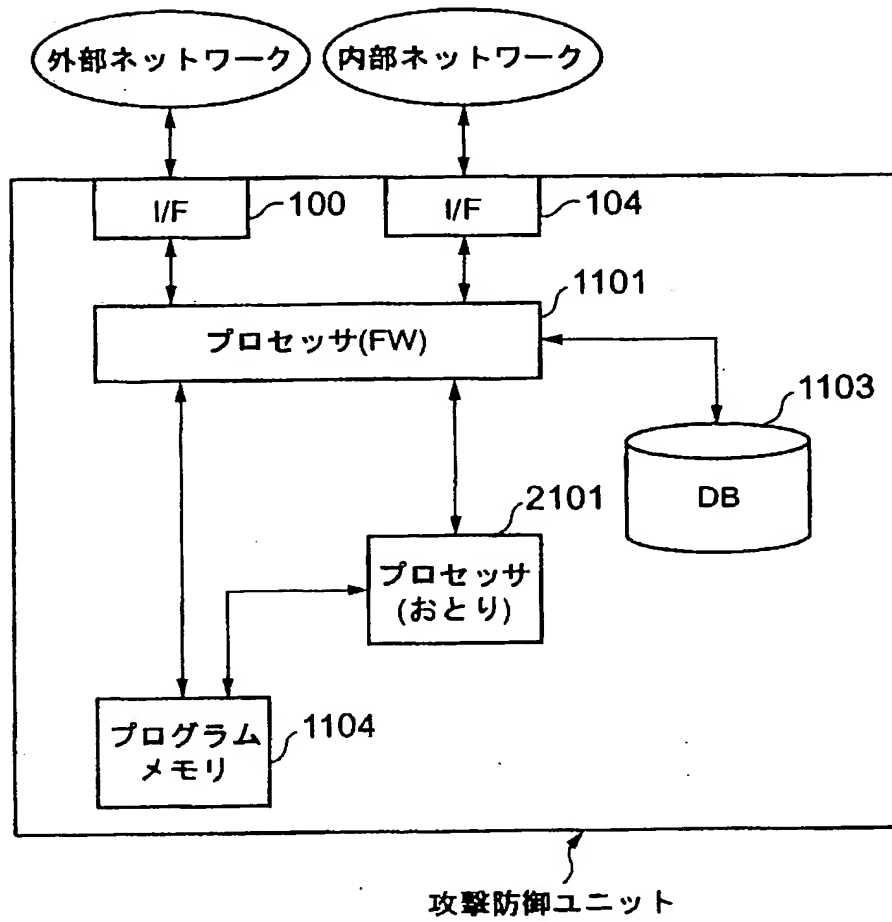
【図53】

要求データ	信頼度
D0	1
D1	0
...	...
Dn	1

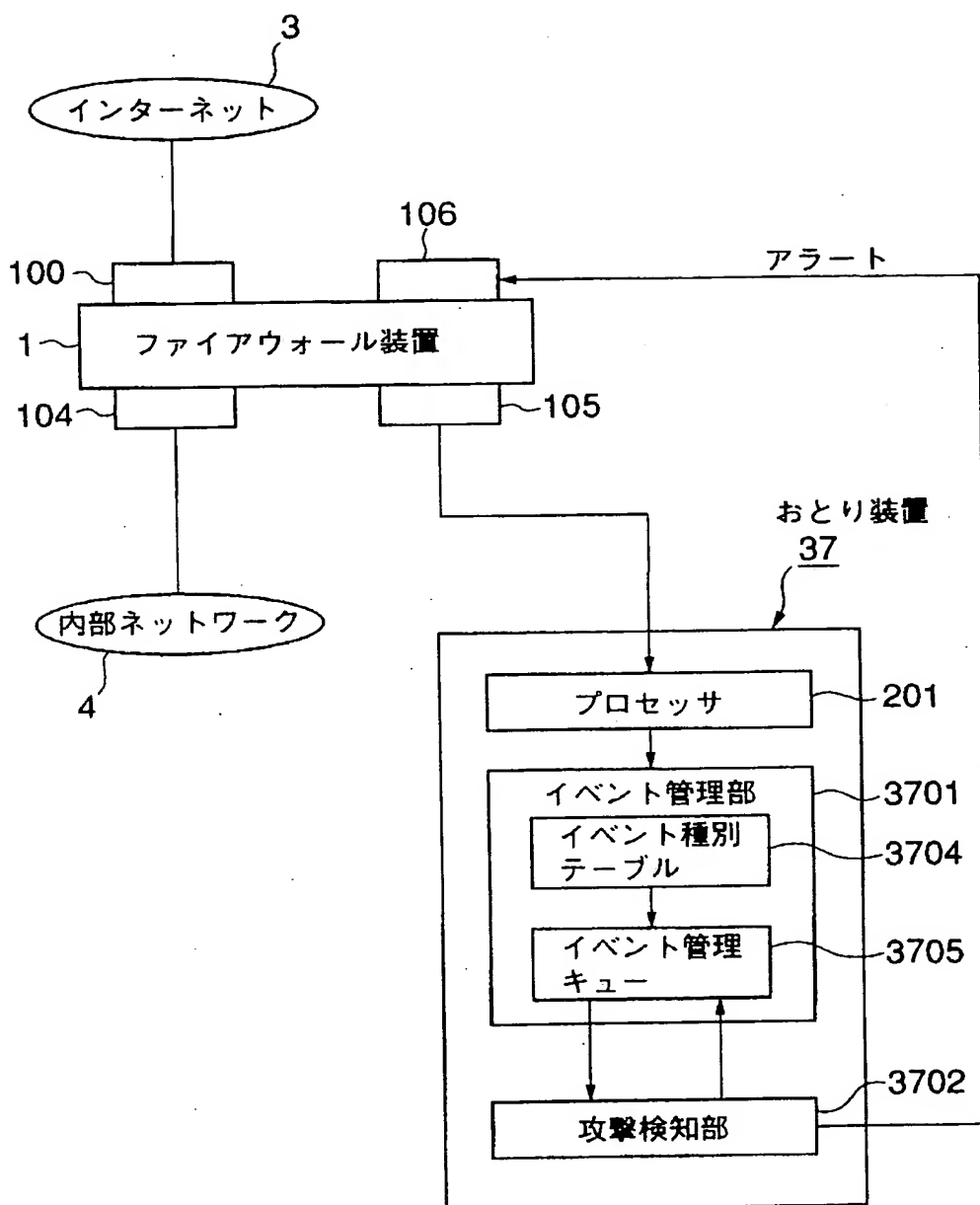
【図31】



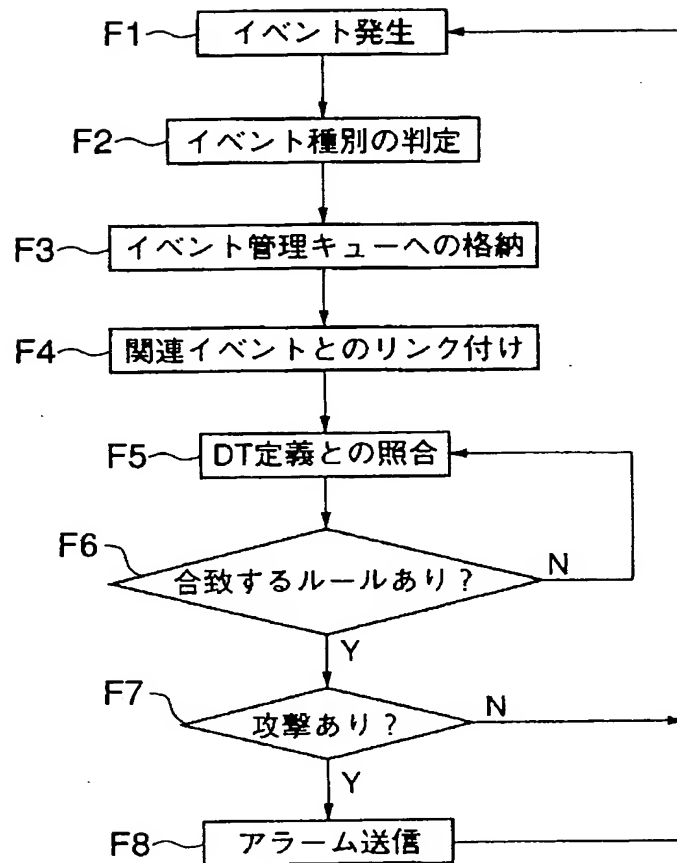
【図32】



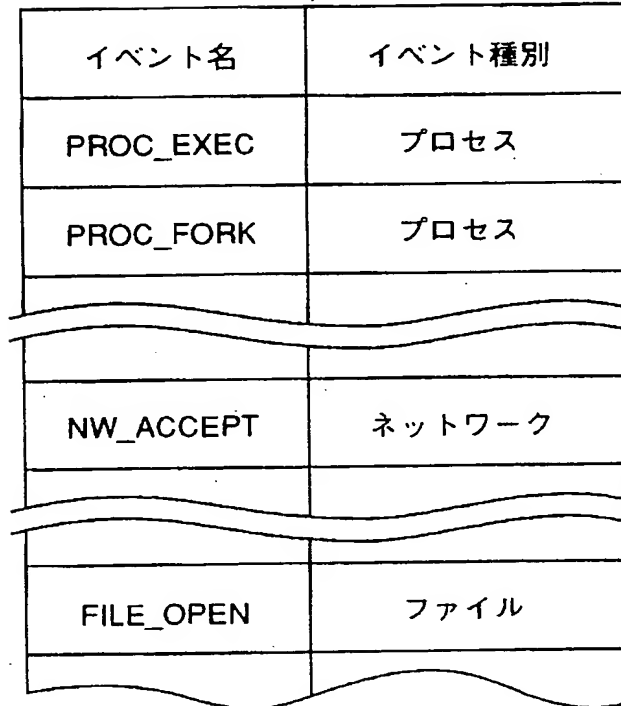
【図33】



【図34】



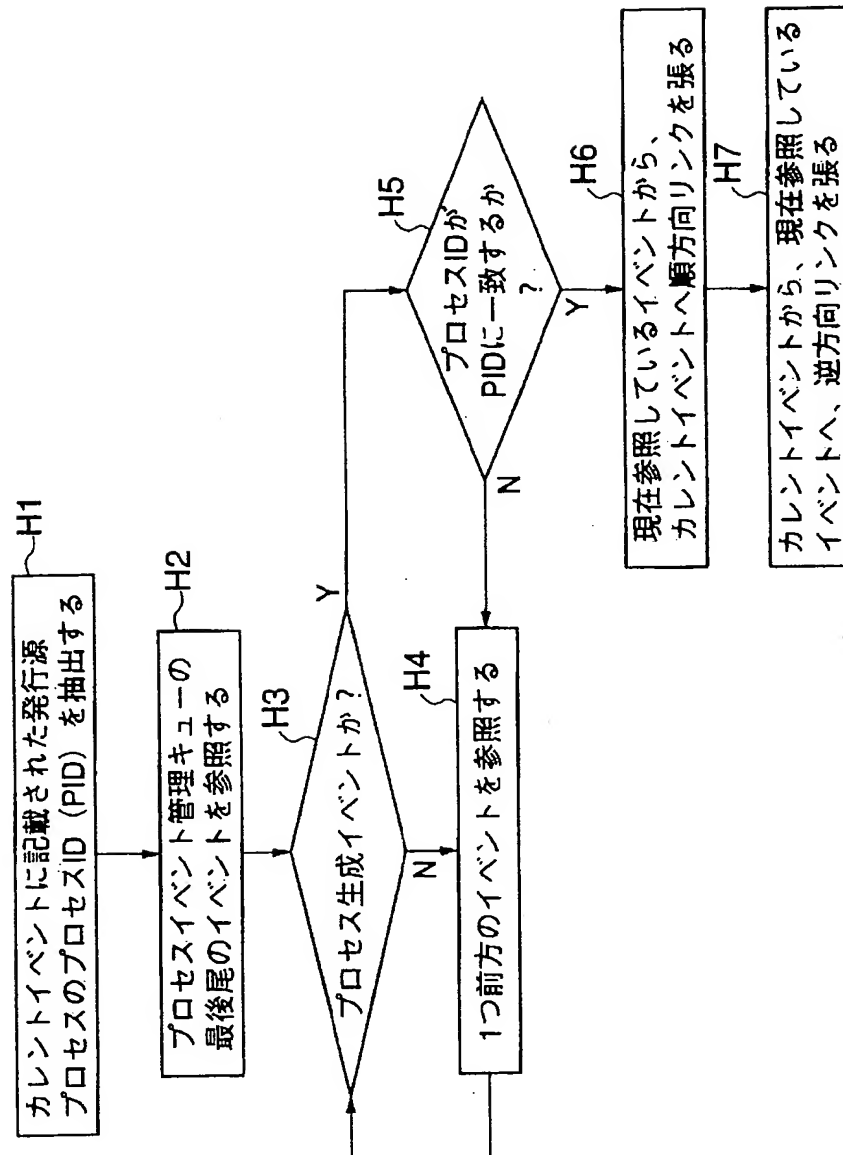
【図35】

イベント種別テーブル  
3704

イベント名	イベント種別
PROC_EXEC	プロセス
PROC_FORK	プロセス
NW_ACCEPT	ネットワーク
FILE_OPEN	ファイル



【図37】



【図39】

## 4101 DT定義ファイル

```
# (ルール1) WWWサーバによるログの書き出しを許可する。
0.0.0.0/0,<inetinfo.exe>,FILE_WRITE,C:\winnt\system32\LogFiles\*;ALLOW
# (ルール2) WWWサーバによるコンテンツ領域の読み込みを許可する。
0.0.0.0/0,<inetinfo.exe>,FILE_READ,C:\inetpub\wwwroot\*;ALLOW

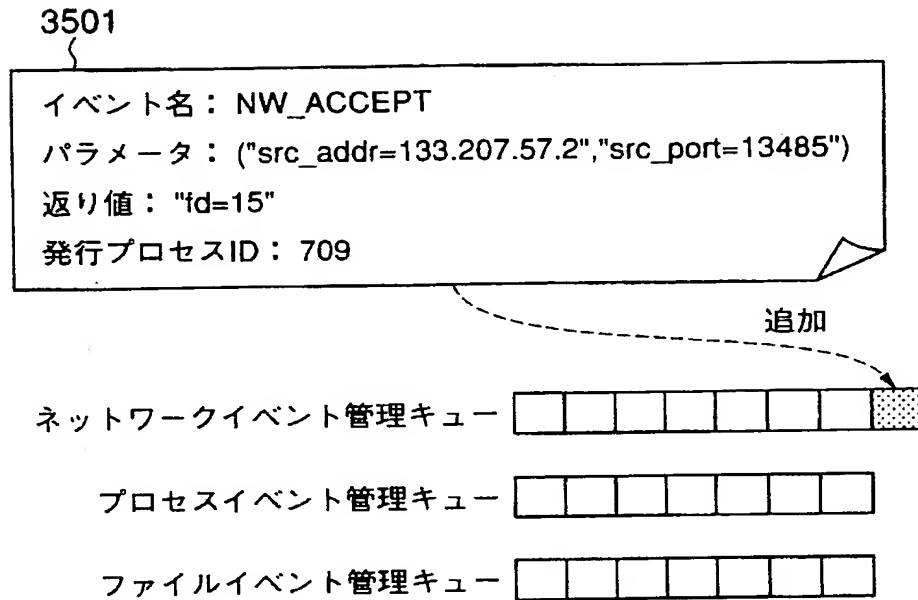
# (ルール3) WWWサーバのサブシステムである登録CGIはデータベースを更新してよい。
0.0.0.0/0,<inetinfo.exe><regist.exe> $,FILE_WRITE,C:\data\client.db;ALLOW
# (ルール4) WWWサーバのサブシステムである出力CGIによるデータベース読み込みを許可。
0.0.0.0/0,<inetinfo.exe><view.exe> $,FILE_READ,C:\data\client.db;ALLOW

# (ルール5) FTPサーバはコンテンツ領域に書き出し可能
# ただし、管理者ドメイン10.56.192.0/24からのアクセスに限る
10.56.192.0/24.^<ftpd.exe>+ $,FILE_WRITE,C:\inetpub\wwwroot\*;ALLOW

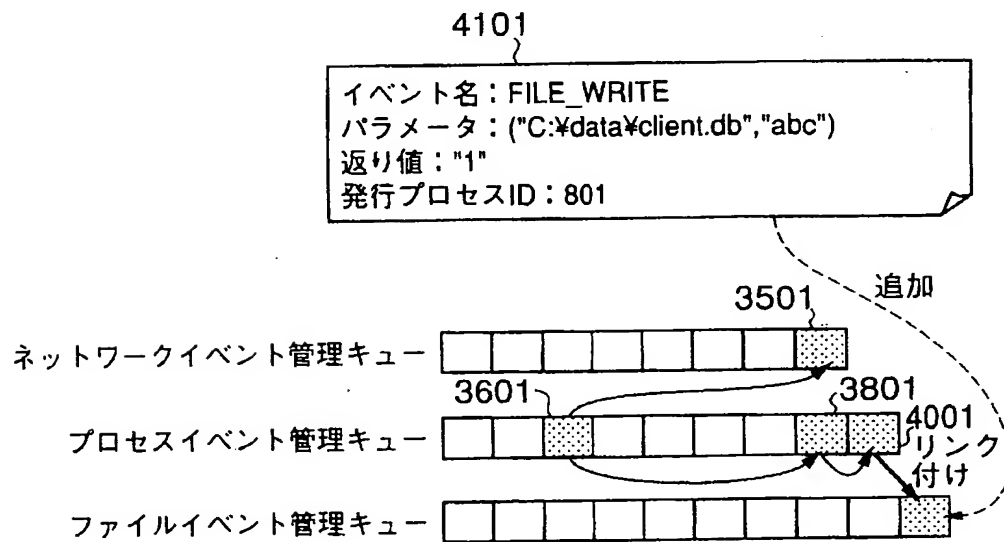
# (ルール6) WWWサーバは、特に許可されていない限り、ファイル書き出しを行わない。
0.0.0.0/0,<inetinfo.exe>.FILE_WRITE,*.DENY
# (ルール7) 許可されたプログラム以外によるデータベース領域のアクセスを禁止する。
0.0.0.0/0,*,*,FILE_READ;FILE_WRITE,C:\data\*.DENY
# (ルール8) 許可されたプログラム以外によるコンテンツ領域の書換えは攻撃である。
0.0.0.0/0,*,*,FILE_WRITE,C:\inetpub\wwwroot\*.DENY

# (デフォルトルール) どのルールにもマッチしない場合は「許可」
DEFAULT;ALLOW
```

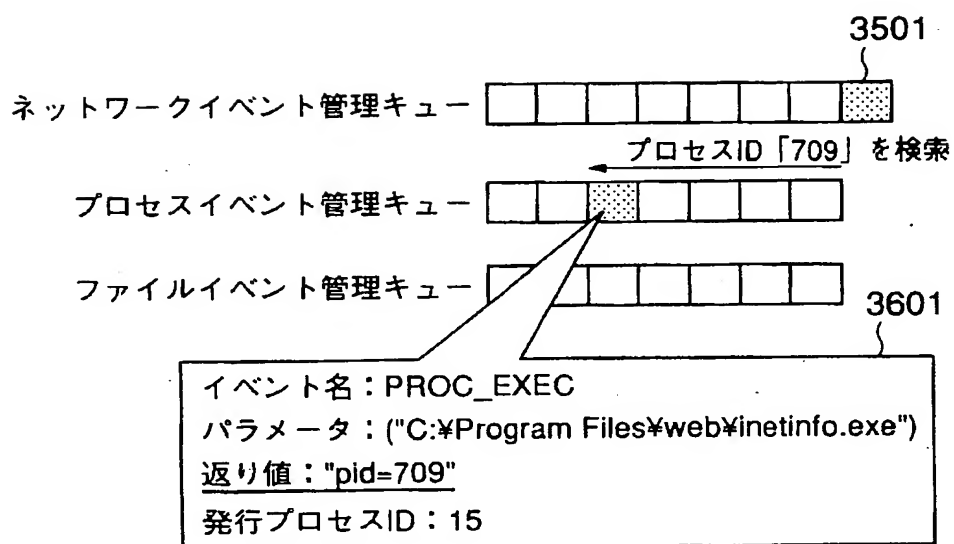
【図41】



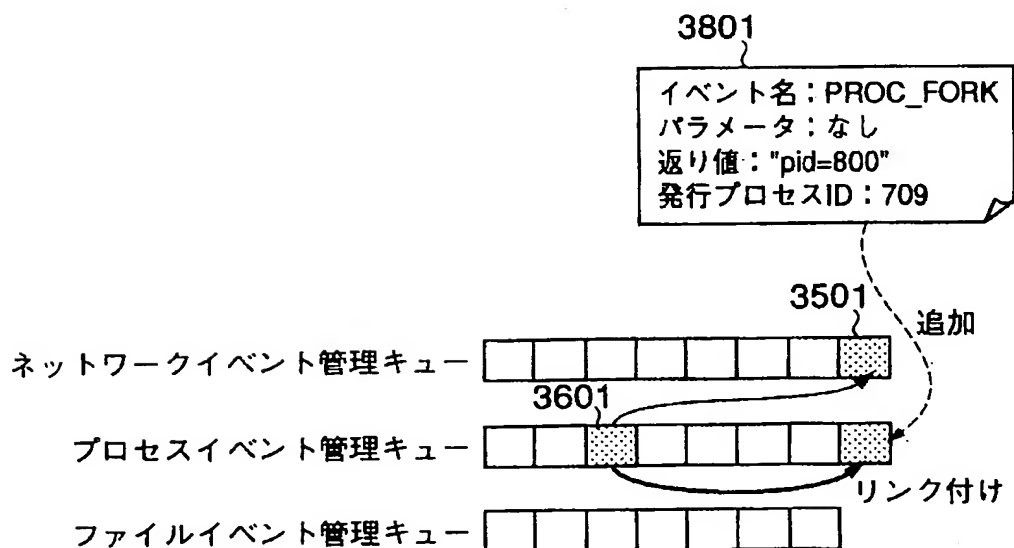
【図47】



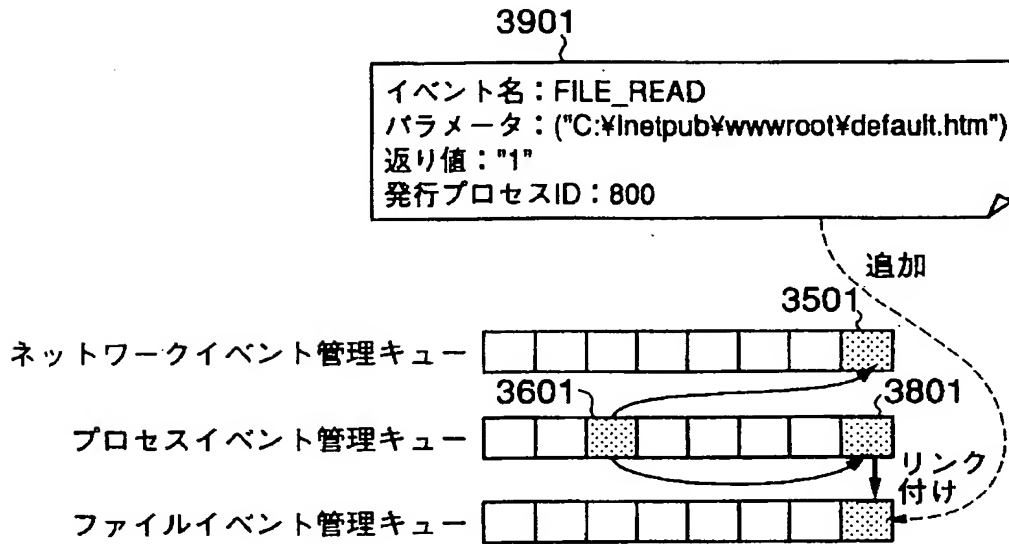
【図42】



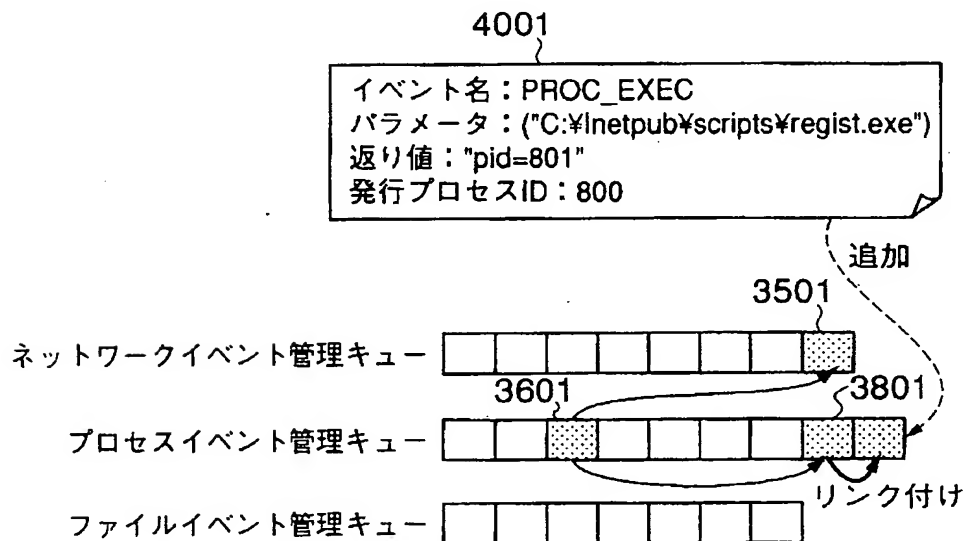
【図44】



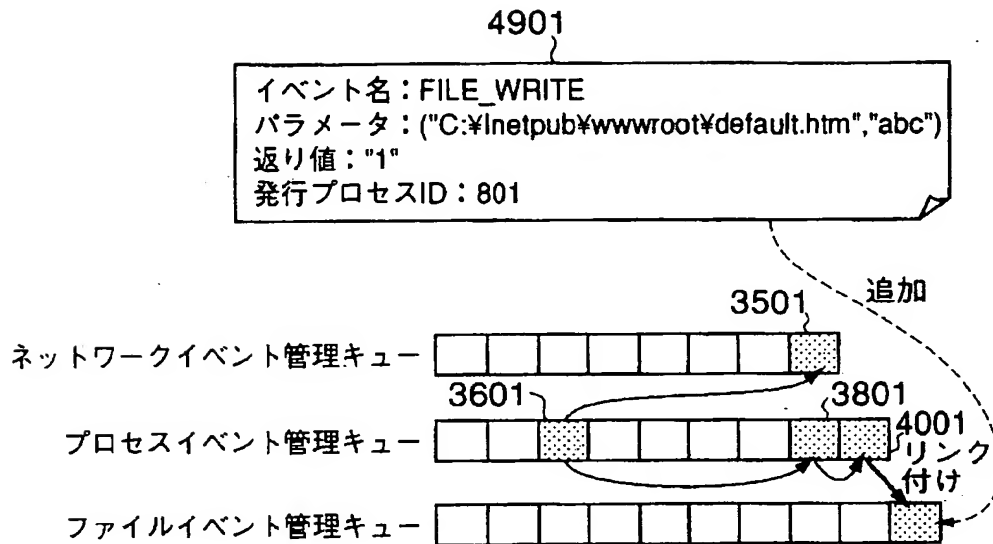
【図45】



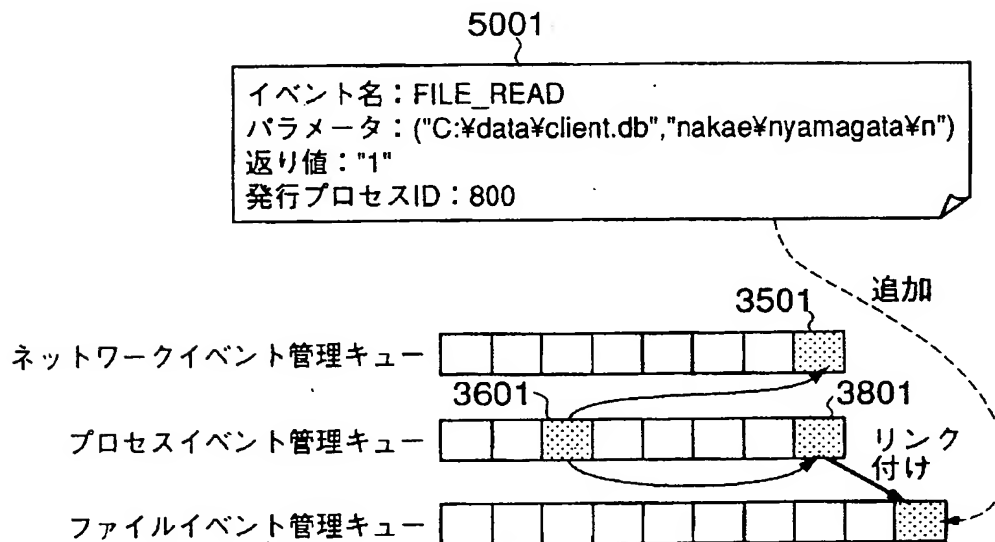
【図46】



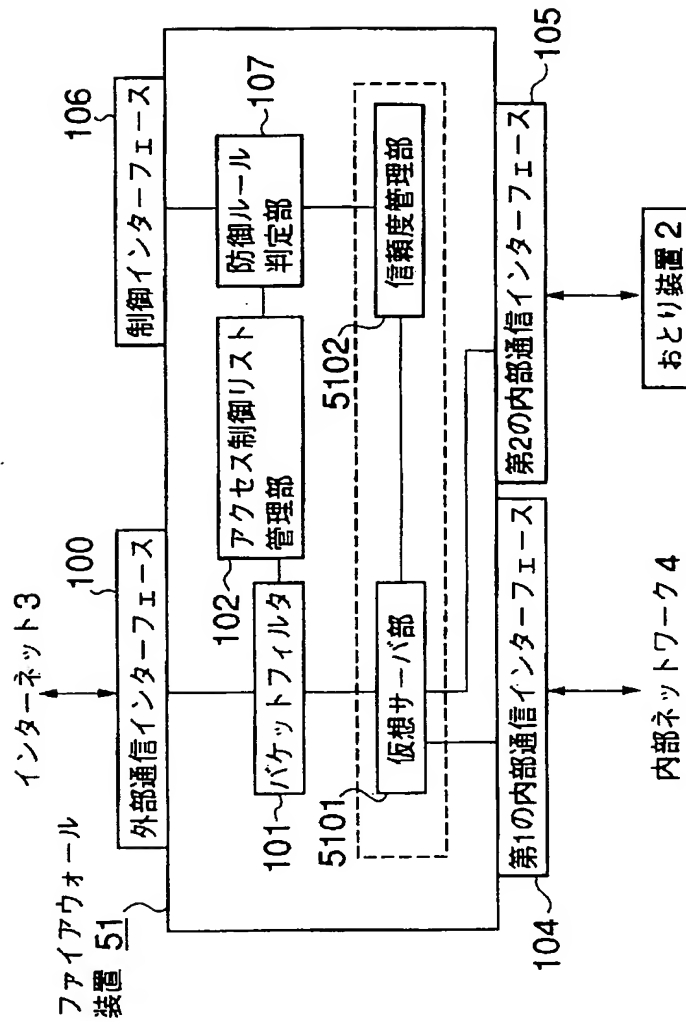
【図48】



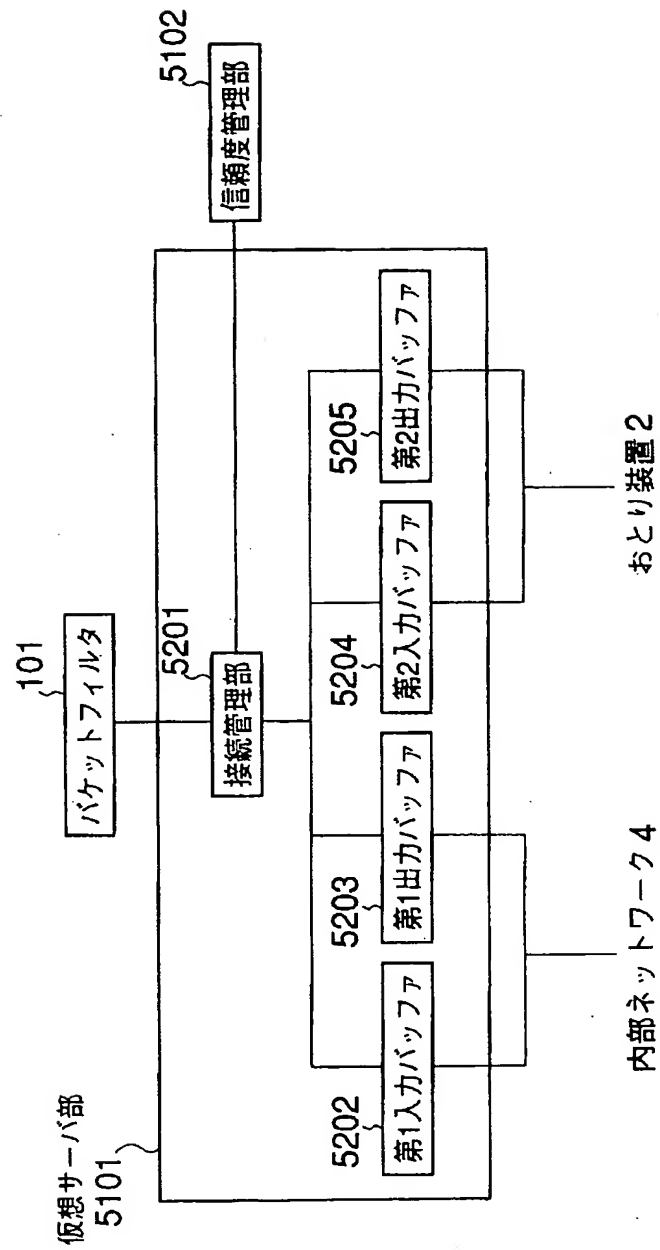
【図49】



【図50】

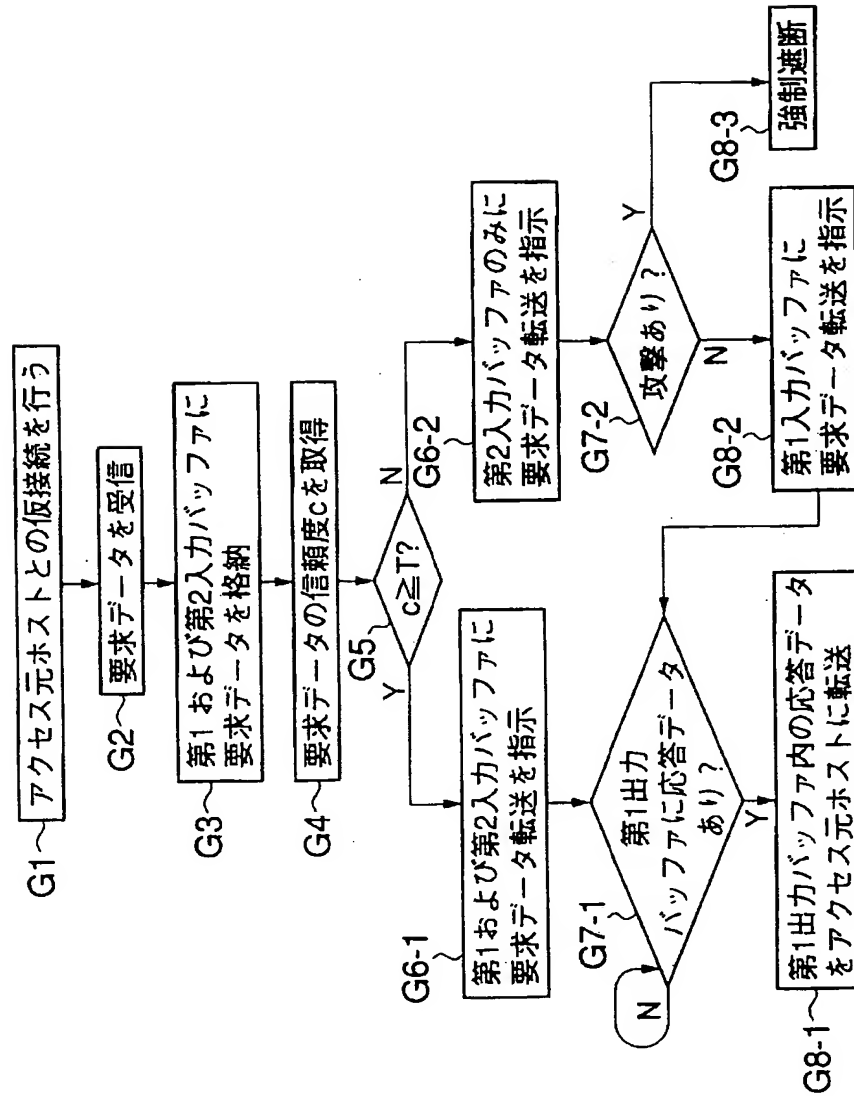


【図51】

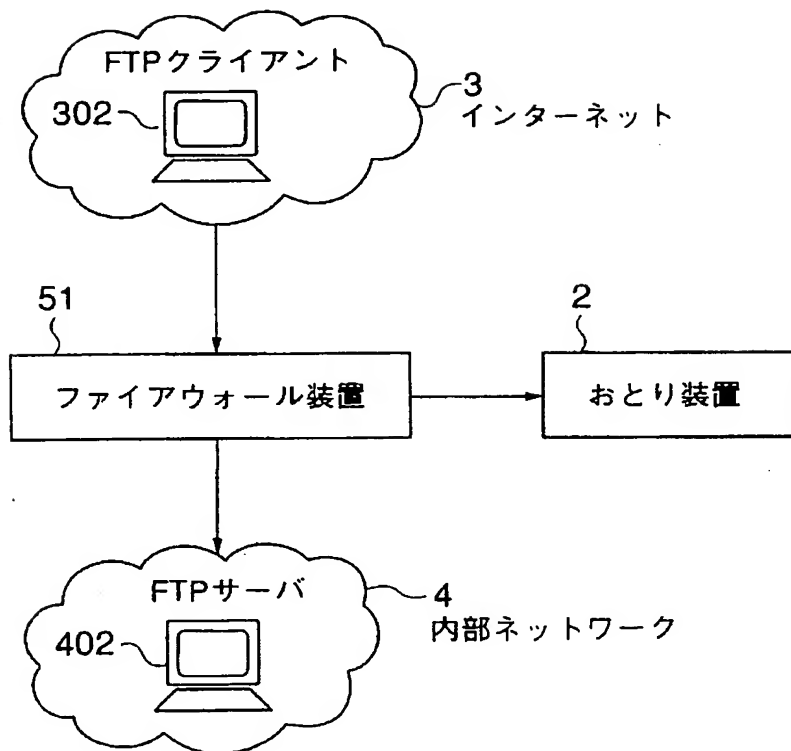




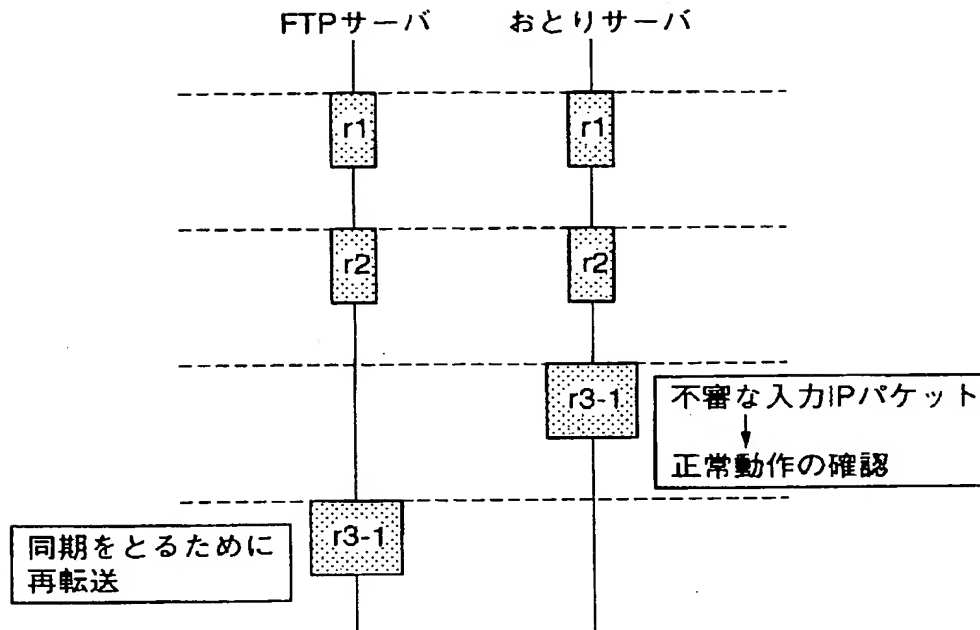
【図52】



【図54】



【図56】

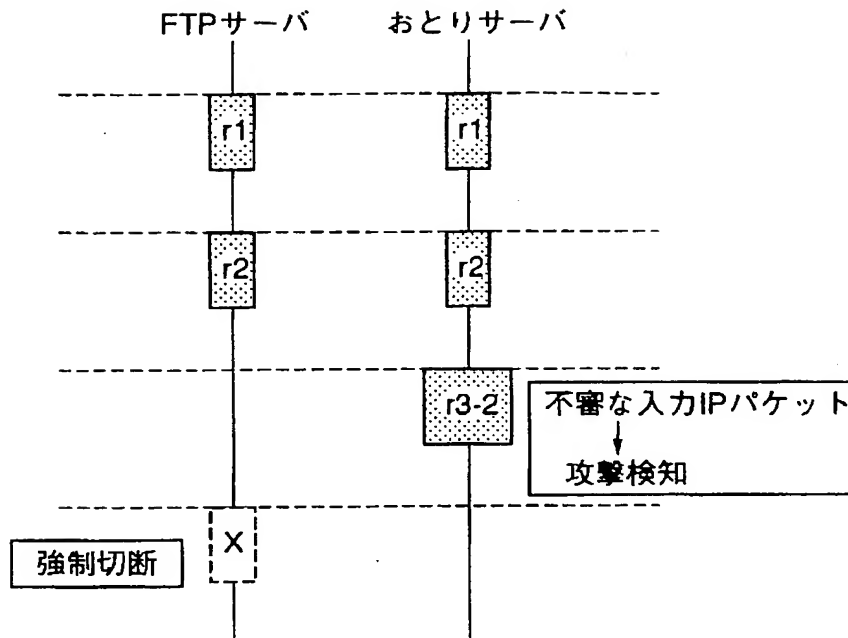


【図62】

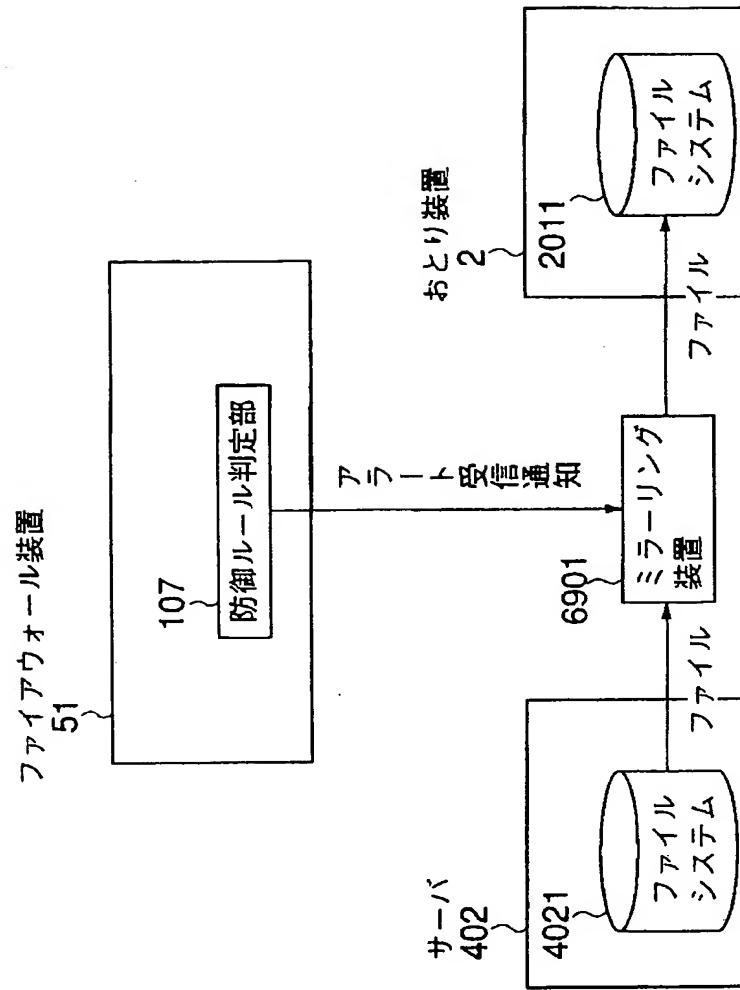
8003 参照表

サーバ識別子	必須信頼度
D1	M1
D2	M2
...	...
Dk	Mk

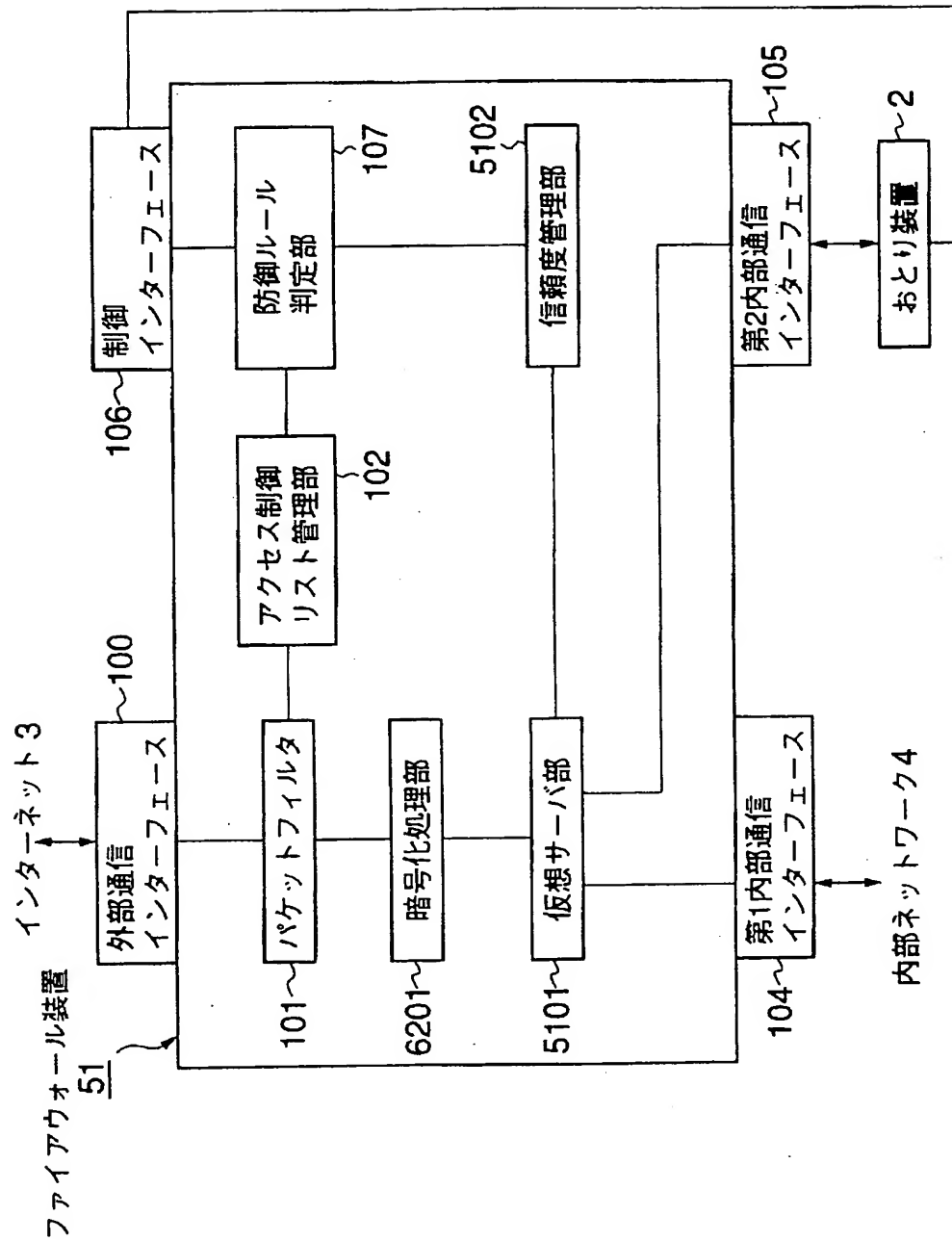
【図57】



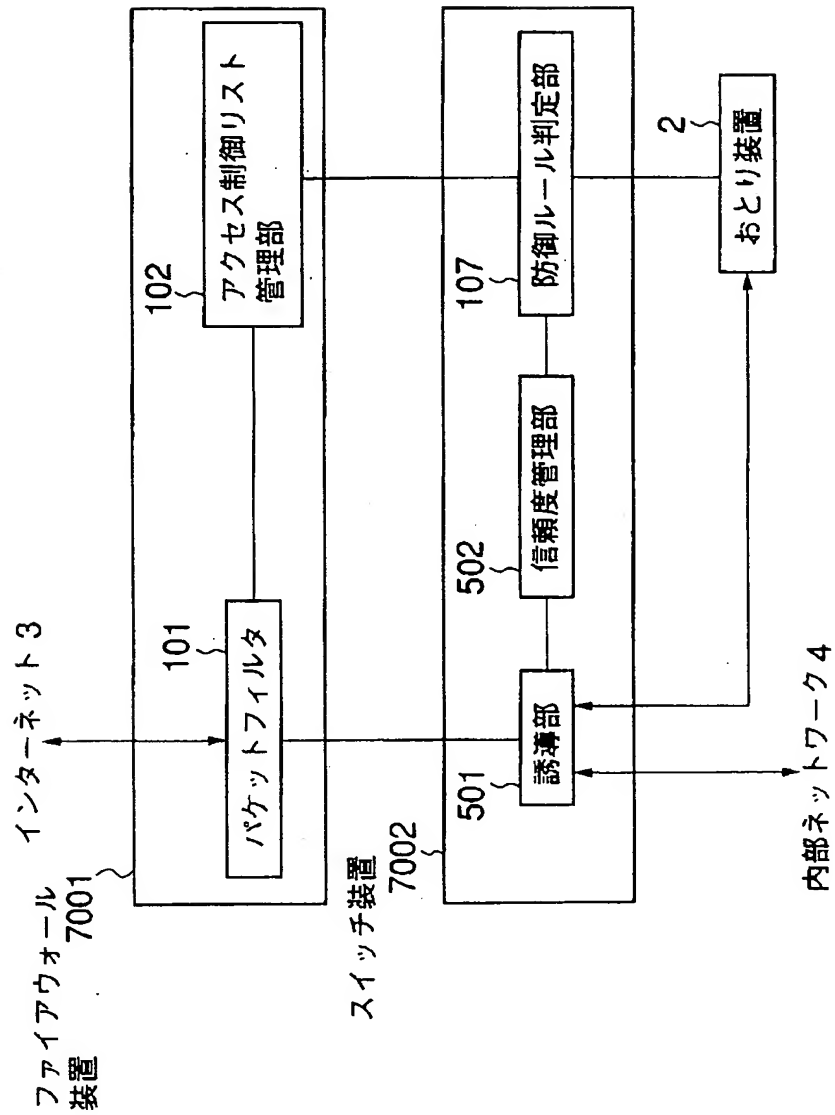
【図58】



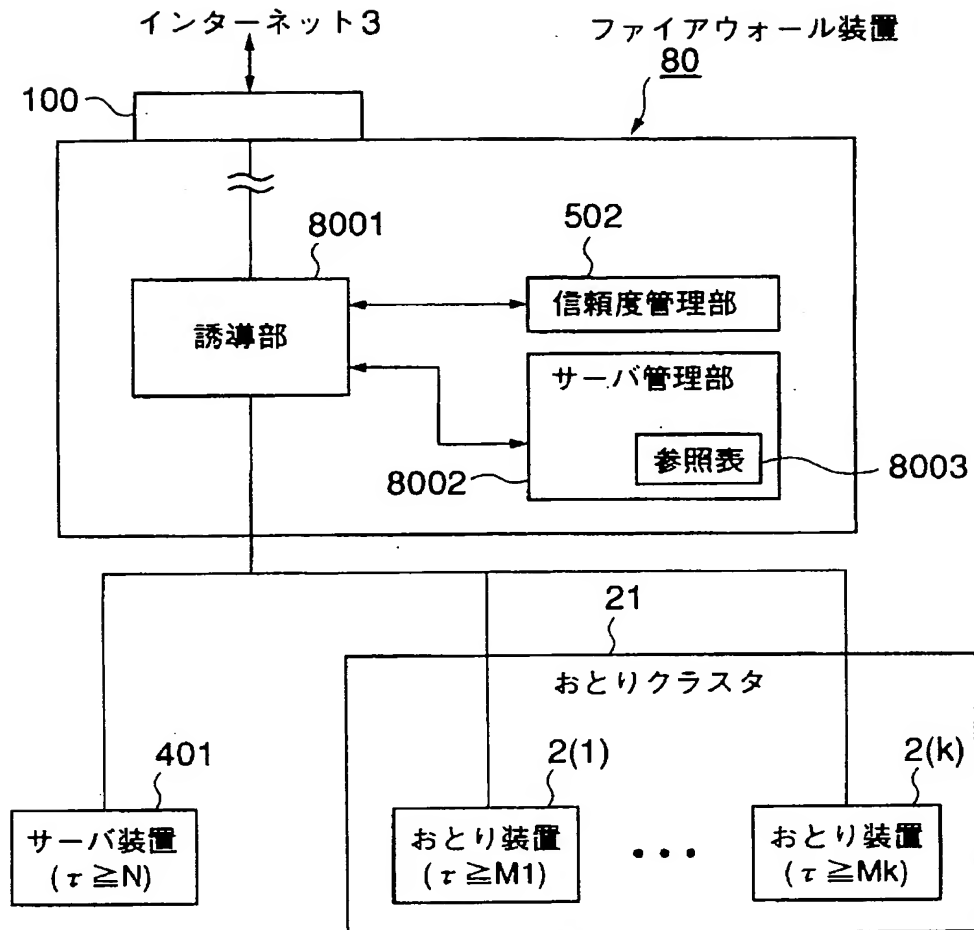
【図59】



【図60】

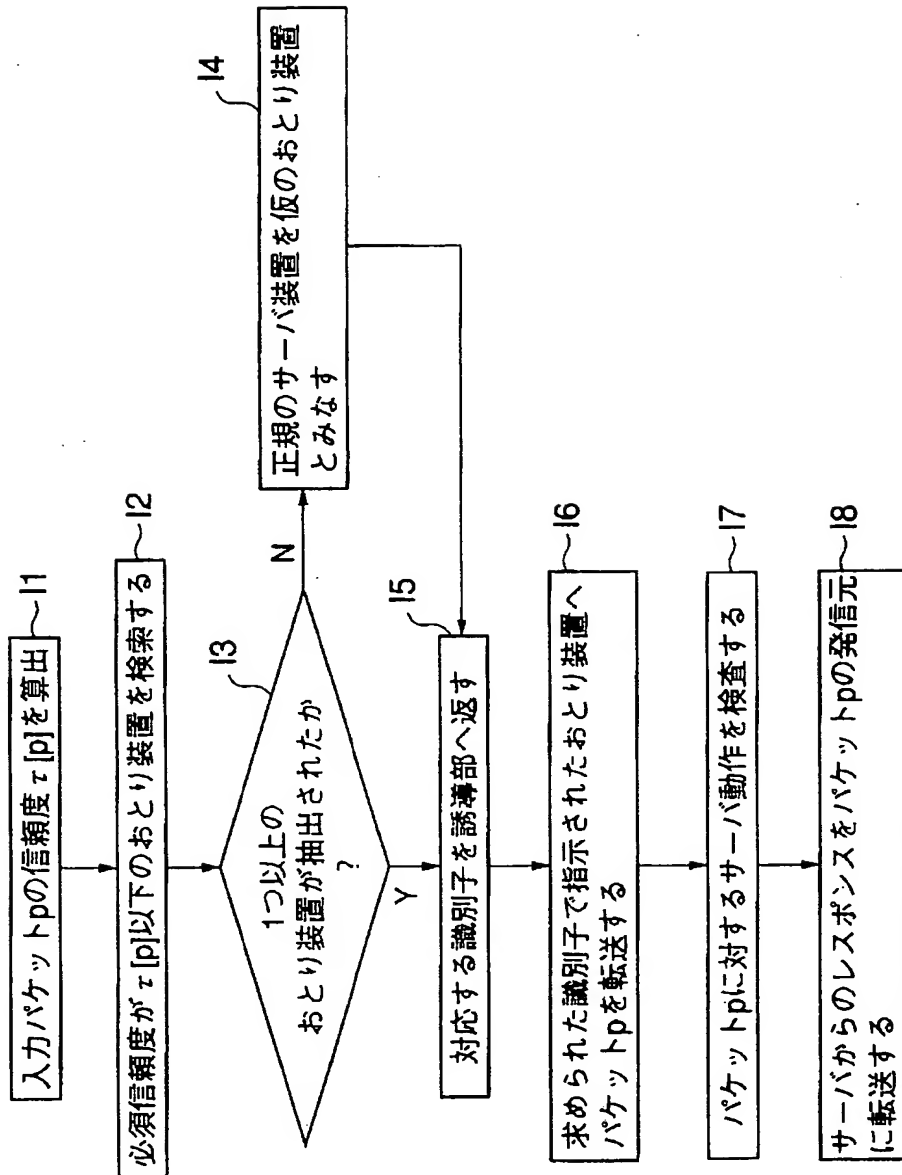


【図61】

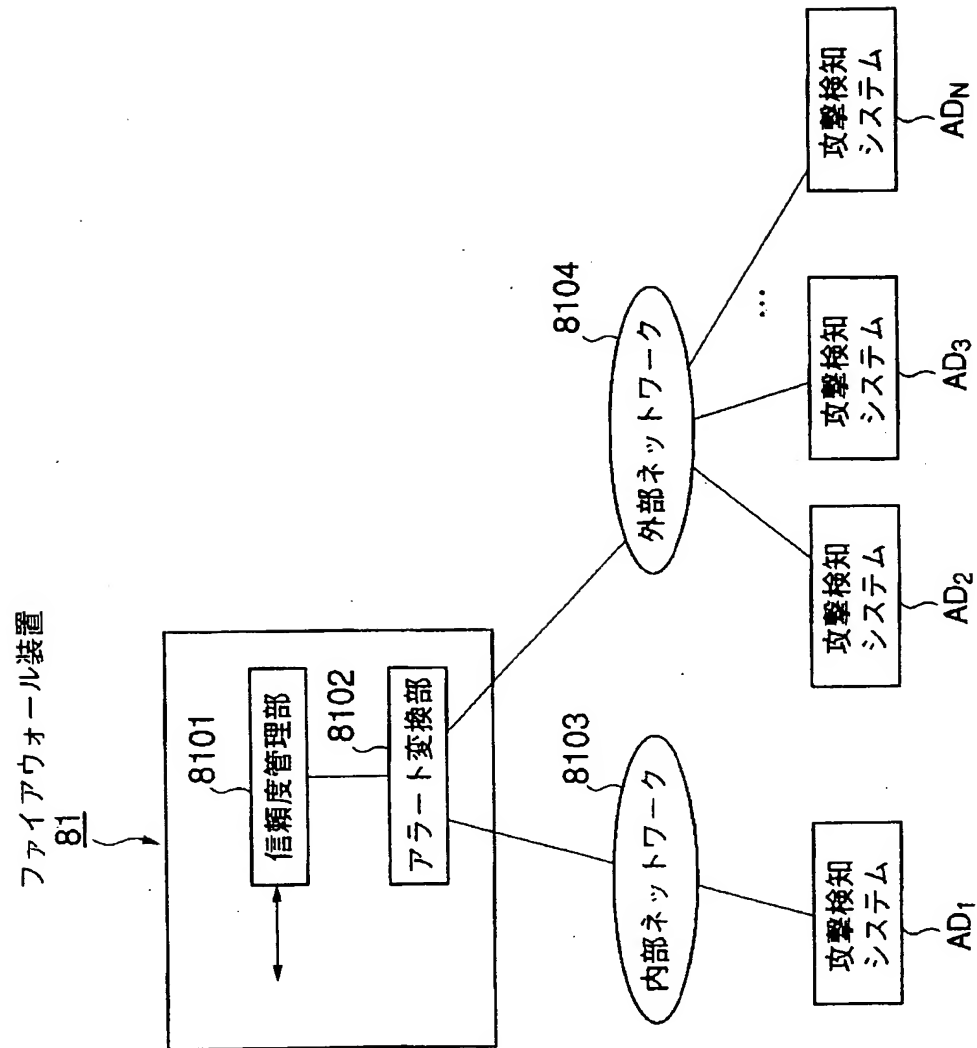




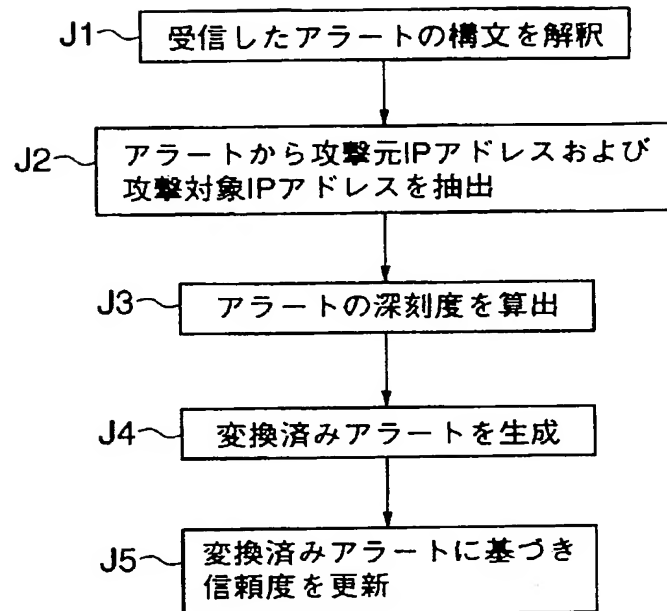
【図63】



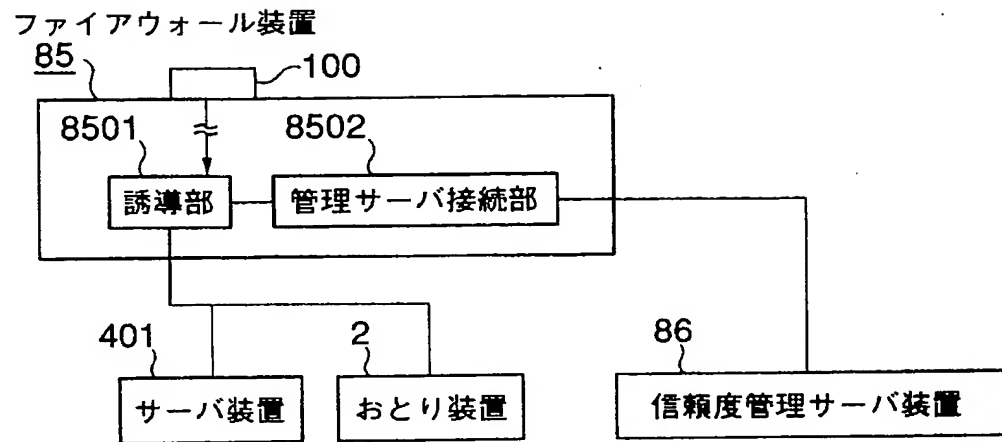
【図64】



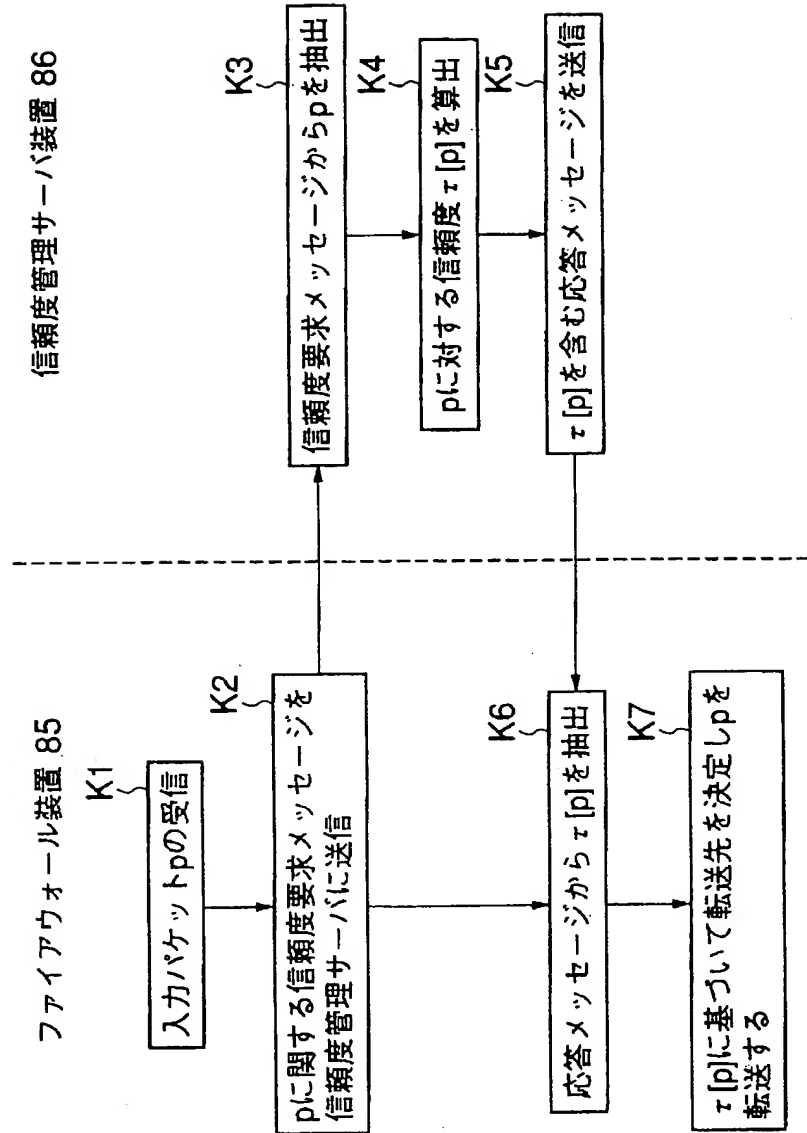
【図65】



【図66】



【図67】



## 【手続補正書】

【提出日】平成15年8月29日(2003. 8. 29)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0234

【補正方法】変更

【補正の内容】

【0234】

続けて、イベント制約の判定を行う。イベント名「FILE\_WRITE」と、イベント3501のイベント名「NW\_ACCEPT」とを照合するが、この場合、一致しないので、当該ルールの照合処理を中断し、次のルール照合へ移る。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0237

【補正方法】変更

【補正の内容】

【0237】

プロセッサ201は、子プロセスの生成動作を受けて、イベント3801(図44参照)をイベント管理部3701に伝達する。イベント3801の内容には、少なくとも、イベント名「PROC\_FORK」と、実行形ファイルのパス名「C:\Web\inetinfo.exe」と、生成された子プロセスのプロセスID(800)と、当該イベントの発生源であるプロセスID(709)が記載される。この他、スレッドと(狭義の)プロセスを区別するためのフラグなどを設けてもよい。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0248

【補正方法】変更

【補正の内容】

【0248】

0.0.0.0/0、<inetinfo.exe>、FILE\_READ、C:\inetinfo\\*、

ALLOW

12.4.2.4) データベース操作

別の要求データの例として、「GET /cgi-bin/regist.exe name=someoneHTTP/1.0」である場合の動作例を示す。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0249

【補正方法】変更

【補正の内容】

【0249】

(ア) CGIの起動

この要求データに対して、前記子プロセスは、まず、前記登録CGIを起動して、新たな孫プロセスを生成す

る。また、URLパラメータ「name=someone」は環境変数「QUERY\_STRING」に格納されているものとする。

## 【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0250

【補正方法】変更

【補正の内容】

【0250】

この動作を受けて、プロセッサ201はイベント4001(図46参照)をイベント管理部3701に伝達する。イベント4001の内容には、少なくとも、イベント名「PROC\_EXEC」と、実行形ファイルのパス名「C:\inetpub\scripts\regist.exe」と、前記孫プロセスのプロセスID(801)と、当該イベントの発生源である前記子プロセスのプロセスID(800)とが記載される。この他、環境変数の情報などを含めてもよい。

## 【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0255

【補正方法】変更

【補正の内容】

【0255】

データベース出力の具体例として、登録CGIは前記環境変数「QUERY\_STRING」の値を読み取り、その値「name=someone」に改行記号を加えた文字列を前記データベースの末尾に追記するものとする。

## 【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0256

【補正方法】変更

【補正の内容】

【0256】

この動作を受けて、プロセッサ201はイベント4101(図47参照)をイベント管理部3701に伝達する。イベント4101の内容には、少なくとも、イベント名「FILE\_WRITE」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記孫プロセスのプロセスID(801)とが記載される。この他、書き出したデータの内容などを含めてもよい。

## 【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0260

【補正方法】変更

【補正の内容】

【0260】

0.0.0.0/0、<inetinfo.exe><regist.exe>\$、FILE\_WRITE、

C:\data\client.db; ALLOW

12.4.3) 動作例2

具体的な動作の別の例として、外部ネットワーク3上のクライアント(133.201.57.2)から、内部ネットワーク4上のWWWサーバに対する不審アクセスがあって、それが攻撃である場合を示す。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0268

【補正方法】変更

【補正の内容】

【0268】

前記不正アクセスがあった場合、前記動作(C-1)が行われ、プロセッサ201はイベント4901(図48参照)をイベント管理部3701に伝達する。イベント4901の内容には、少なくとも、イベント名「FILE\_WRITE」と、実行形ファイルのパス名「C:\inetpub\wwwroot\default.htm」と、当該イベント発生源である前記孫プロセスのプロセスID(801)とが記載される。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0272

【補正方法】変更

【補正の内容】

【0272】

0.0.0.0/0、<inetinfo.exe>、FILE\_WRITE、.\*; DENY

そして、攻撃検知部3702は、攻撃元ホスト「133.201.57.2」を含むアラームを直ちに生成して、前記ファイアウォール装置1へ送信する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0274

【補正方法】変更

【補正の内容】

【0274】

また、WWWサーバ以外のサーバ、例えばFTPサーバを介したコンテンツ領域への書き込みがあった場合、以下のルール(図39のルール5)に合致しない限り、すなわち、管理ドメインからの正当な保守作業でない限り、

10.56.192.0/24、<ftpd.exe>+\$. FILE\_WRITE、C:\inetpub\wwwroot\.\*; ALLOW

以下のルール(図39のルール8)により、攻撃であると判定される。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0275

【補正方法】変更

【補正の内容】

【0275】

0.0.0.0/0、.\*、FILE\_WRITE、C:\inetpub\wwwroot\.\*; DENY

12.4.3.2) データベースへの不正アクセス  
WWWサーバまたはそのサブシステム(登録CGI・出力CGI)などに脆弱性が存在するものとし、「GET/cgi-bin/..%c1%c9../data/client.db HTTP/1.0」というアクセスによって、前記顧客データベースを窃取されるものとする。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0276

【補正方法】変更

【補正の内容】

【0276】

前記不正アクセスがあった場合、前記動作が行われたのを受けて、プロセッサ201はイベント5001(図49参照)をイベント管理部3701に伝達する。イベント5001の内容には、少なくとも、イベント名「FILE\_READ」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記子プロセスのプロセスID(800)とが記載される。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0280

【補正方法】変更

【補正の内容】

【0280】

0.0.0.0/0、.\*、FILE\_READ|FILE\_WRITE、C:\data\.\*; DENY

そして、攻撃検知部3702は、攻撃元ホスト「133.201.57.2」を含むアラームを直ちに生成して、前記ファイアウォール装置1へ送信する

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**